This Issues Paper reflects the law as at 20 September 2006

ISBN-0-9758213-6-9

Commission Reference: IP 31

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 Canprint Communications 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 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 submisions are made available during the Inquiry to other state and territory law reform bodies working on a privacy inquiry. Non-confidential submissions are also made available to any other 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
E-mail: privacy@alrc.gov.au

Submissions may also be made using the on-line form on the ALRC's homepage: <www.alrc.gov.au>.

The closing date for submissions in response to IP 31 is Monday 15 January 2007.

Contents

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)
Mr Brian Opeskin (Deputy President)
Associate Professor Les McCrimmon (Commissioner)
Justice Robert French (part-time Commissioner)
Justice Susan Kenny (part-time Commissioner)
Justice Susan Kiefel (part-time Commissioner)

Senior Legal Officers

Carolyn Adams
Bruce Alston
Kate Connors
Isabella Cosenza
Jonathan Dobinson

Legal Officers

Althea Gibson
Lauren Jamieson
Huette Lam
Peter Turner (until August 2006)
Edward Santow

Research Manager

Lani Blackman

Librarian

Carolyn Kearney

Project Assistants

Alayne Harland
Tina O'Brien

Legal Interns

Mr Justin Carter
Ms Elizabeth Crook
Mr Joash Dache
Ms Maggie Fung
Ms Dawnie Lam
Ms Fiona Roughley
Ms Teneille Steptoe
Ms Michelle Tse
Ms 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)
Ms Karen Curtis, Privacy Commissioner (Cth)
Mr Peter Ford, Privacy, Security and Telecommunications Consultant
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
Dr Moira Paterson, Faculty of Law, Monash University
Ms Joan Sheedy, Australian Attorney-General's Department
Mr Peter Shoyer, Information Commissioner (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)

Health Sub Advisory 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 Questions

1. Introduction to the Inquiry

1–1 Should the *Privacy Act* be amended to provide direct protection to groups such as: (a) Indigenous or other ethnic groups; or (b) commercial entities? If so, which groups or commercial entities should be covered by the Act?

1–2 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?

2. Overview of Privacy Regulation in Australia

2–1 Is national consistency in the regulation of personal information important? If so, what are the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia?

3. The *Privacy Act 1988* (Cth)

3–1 Is the structure of the *Privacy Act* logical? Does the *Privacy Act* need to be redrafted to achieve a greater degree of simplicity and clarity?

3–2 Insofar as the *Privacy Act* is primarily concerned with data protection, is the name of the *Privacy Act* accurate and appropriate?

3–3 Is there some benefit in amending the *Privacy Act* to include the objects of the legislation? If so, what should be included in the objects clause?

3–4 Are the definitions in the *Privacy Act* adequate and appropriate? For example, are the definitions of 'personal information' and 'sensitive information' in the *Privacy Act* adequate and appropriate?

3–5 Should the definition of 'personal information' in the *Privacy Act* be amended to include personal information of the deceased?

4. Examination of the Privacy Principles

4–1 Are the obligations imposed on **organisations** at the time of collection of personal information adequate and appropriate? For example, should an organisation also be required to make an individual aware of (a) the types of people, bodies or agencies to whom the organisation usually discloses information of that kind; (b) the various avenues of complaint available; and (c) the source of the information, where it has not been collected directly from the individual?

4–2 Should NPP 1 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 aware of specified matters relating to the collection of personal information?

4–3 Are the obligations imposed on **agencies** at the time of collection of personal information adequate and appropriate? In particular, should agencies also be subject to a general requirement that where reasonable and practicable, they should collect information about an individual only from the individual concerned? Should agencies also be required to notify an individual of his or her rights of access to the information, the consequences of not providing the information, the various avenues of complaint available, and the source of the information, where it has not been collected directly from the individual?

4–4 Should any obligations attach to an agency or organisation which receives unsolicited personal information that it intends to include in a record or generally available publication? If so, what obligations should be imposed?

4–5 Should the obligations imposed on an organisation or agency at or soon after collection apply irrespective of the source of personal information?

4–6 Is it desirable for the IPPs to deal separately with the principles relating to the use and disclosure of personal information or should use and disclosure be provided for in one principle?

4–7 Are the circumstances in which agencies and organisations are permitted to use and disclose personal information under IPPs 10 and 11, and NPP 2, adequate and appropriate? In particular, should agencies and organisations be permitted expressly to disclose personal information: (a) to assist in the investigation of missing persons; (b) 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; and (c) in times of emergency? What mechanism should be adopted to establish the existence of an emergency?

4–8 Are the criteria in NPP 2.1(a) for using personal sensitive and non-sensitive information for a secondary purpose adequate and appropriate? For example, is it necessary or desirable that there also be a 'direct' relationship between the secondary and primary purpose of collection before non-sensitive personal information can be used or disclosed for a secondary purpose?

4–9 Is the scope of IPP 10(e) (which allows agencies to use personal information for a purpose other than the particular purpose of collection, if the purpose for which the information is used is directly related to the purpose of collection) adequate and appropriate? For example, should there be an additional requirement that the individual concerned would reasonably expect an agency to use the information for that other purpose?

4–10 In what circumstances should agencies or organisations be required to record their use or disclosure of personal information when it is used or disclosed for a purpose other than the primary purpose?

4–11 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?

4–12 Is it appropriate that NPP 2 allows for personal non-sensitive information to be used for the secondary purpose of direct marketing? If so, are the criteria that an organisation needs to satisfy in order to use personal information for direct marketing purposes adequate and appropriate?

4–13 Should use and disclosure of personal information be allowed for research that does not involve health information—for example social science research? If so, in what circumstances or upon what conditions might this be appropriate?

4–14 Is the scope of the data quality principle in NPP 3 (which requires 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) adequate and appropriate? For example, should the principle expressly apply to information that an organisation controls?

4–15 Is there a need to amend NPP 3 to clarify the extent of the obligations of an organisation under the data quality principle or is this best dealt with by way of guidance issued by the Office of the Privacy Commissioner?

4–16 Should agencies be subject to a stand-alone data quality principle that extends to the collection, use and disclosure of personal information?

4–17 Is the scope of NPP 4 relating to the obligations of an organisation to secure data adequate and appropriate? For example, should NPP 4 be amended to impose an obligation on organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected?

4–18 Are there any circumstances in which agencies should be under an obligation to destroy or permanently de-identify personal information when it is no longer needed?

4–19 Should the IPPs and the NPPs regulate the deletion of personal information by organisations and agencies? In what circumstances might this be appropriate? Should an individual have the right to request that an agency or organisation destroy personal information that it holds or controls concerning the individual? If so, in what circumstances or upon what conditions should this be permitted?

4–20 Is the scope of NPP 5 relating to openness adequate and appropriate? For example, is it necessary or desirable for organisations to be given greater legislative guidance about their obligations under the principle? Does the more prescriptive approach to the openness principle in IPP 5 provide a suitable model?

4–21 Is it appropriate that certain obligations under the NPPs relating to openness are triggered only upon an individual's request?

4–22 Is there a need to clarify the relationship between the obligation of an organisation under NPP 1.3 (which imposes an obligation on organisations to take reasonable steps to ensure that an individual is aware of specified matters at or before the time of collection) and NPP 5.1 (which imposes an obligation on organisations to set out in a document clearly expressed policies on its management of personal information)? If so, how is this best achieved?

4–23 Are the circumstances in which organisations can deny an individual access to his or her personal information under NPP 6 adequate and appropriate? If the circumstances are inadequate, should this be addressed by legislative amendment to the principle or by guidance issued by the Office of the Privacy Commissioner?

4–24 Should IPP 6 more clearly set out the circumstances in which agencies can deny an individual access to his or her personal information? If so, what circumstances should be included?

4–25 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?

4–26 Is there a need for a separate privacy principle regulating the adoption, collection, use and disclosure of identifiers by organisations? Should NPP 7, the principle regulating identifiers, be redrafted to deal more generally with the issue of data-matching?

4–27 Is the definition of identifier adequate and appropriate? Are the exceptions to the use and disclosure of identifiers referred to in NPP 7 adequate and appropriate? Should an individual be permitted to consent to the use of his or her unique identifier? If so, in what circumstances and by what means should this exception be given effect?

4–28 Should the *Privacy Act* be amended to regulate the assignment, adoption, collection, use and disclosure of identifiers by agencies?

4–29 Should NPP 8, the anonymity principle, be redrafted to impose expressly an obligation on organisations to give an individual the option of remaining anonymous when entering into transactions with those organisations?

4–30 Is it appropriate or desirable for agencies to be subject to an anonymity principle? In what circumstances, if any, might this be appropriate?

4–31 Should the transfer of personal information offshore by agencies be regulated by privacy principles?

4–32 Should federal privacy principles allow agencies and organisations to collect non-health related sensitive information for other purposes, including research and statistical purposes? If so, in what circumstances should this be permitted?

4–33 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?

4–34 Should the *Privacy Act* provide a uniform set of privacy principles that are to apply to both the public (currently covered by the IPPs) and private (currently covered by the NPPs) sectors? If so, what model should be used? Are there any particular principles or exceptions to principles that should apply only to either the public or private sector?

4–35 Apart from the principles contained in the IPPs and NPPs, are there any other principles to which agencies and organisations should be subject? For example, should the IPPs and NPPs include expressly: an 'accountability' principle; a 'prevention of harm' principle; a 'consent' principle; or a requirement that agencies and organisations notify persons whose personal information has been, or is reasonably believed to have been, accessed without authorisation? If so, what should be the content of these principles?

4–36 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?

5. Exemptions from the *Privacy Act 1988* (Cth)

5–1 Is it appropriate for certain entities to be exempt, either completely or partially, from the operation of the *Privacy Act*? If so, where should the exemptions be located?

5–2 Should the following defence and intelligence agencies be exempt, either completely or partially, from the *Privacy Act*:

- Defence Imagery and Geospatial Organisation;
- Defence Intelligence Organisation;
- Defence Signals Directorate;
- Australian Security Intelligence Organisation;
- Australian Secret Intelligence Service; and
- Office of National Assessments?

If so, what is the policy justification for the exemption? Are there any other defence and intelligence agencies that should be exempt, either completely or partially, from the *Privacy Act*?

5–3 Should the following agencies be exempt, either completely or partially, from the *Privacy Act*:

- Australian Government ministers;
- federal courts;

- agencies specified in Schedule 1 to the *Freedom of Information Act 1982* (Cth)—namely, the Australian Industrial Relations Commission, the Australian Fair Pay Commission, the Industrial Registrar and Deputy Industrial Registrars;
- Australian Crime Commission;
- royal commissions;
- Integrity Commissioner;
- agencies specified in Schedule 2 Part I Division 1 of the *Freedom of Information Act 1982* (Cth) other than the intelligence agencies, the Australian Government Solicitor and the Australian Industry Development Corporation; and
- agencies specified in Schedule 2 Part II Division 1 of the *Freedom of Information Act 1982* (Cth)?

If so, what is the policy justification for the exemption? Are there any other agencies that should be exempt, either completely or partially, from the *Privacy Act*?

5–4 Should state and territory authorities be exempt from the privacy principles in the *Privacy Act*?

5–5 In addition to the energy distributors owned by the New South Wales Government, which are the only state authorities prescribed under the *Privacy (Private Sector) Regulations 2001* (Cth), are there any other state or territory authorities that should be covered by the privacy principles in the *Privacy Act*? If so, to what extent should they be covered?

5–6 Should the small business exemption remain? If so: (a) what should be its extent; and (b) should an opt-in procedure continue to be available?

5–7 Should registered political parties be exempt from the operation of the privacy principles in the *Privacy Act?*

5–8 Should political acts and practices be exempt from the operation of the *Privacy Act*? If so, does the current exemption under s 7C of the *Privacy Act* strike an appropriate balance between the protection of personal information and the implied freedom of political communication?

5–9 Should the employee records exemption remain? If so: (a) what should be the scope of the exemption; and (b) should it be located in the *Privacy Act*, workplace relations legislation or elsewhere?

5–10 Should acts and practices of media organisations in the course of journalism be exempt from the operation of the *Privacy Act*? If so: (a) what should be the scope of the exemption; and (b) does s 7B(4) of the *Privacy Act* strike an appropriate balance between the free flow of information to the public and the protection of personal information?

5–11 Should the terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' be defined in the *Privacy Act*? If so, how should they be defined? Are there other terms that would be more appropriate?

5–12 If the media exemption is retained, how should journalistic acts and practices be regulated?

5–13 Do any issues arise concerning related bodies corporate, changes in partnership and overseas acts required by foreign law in Part III Division 1 of the *Privacy Act*? If so, how should they be dealt with?

5–14 Are there any other entities or types of activities that should be exempt from the operation of the *Privacy Act*? If so, what are those entities or types of activities, and what should be the scope of the exemption?

6. Powers of the Office of the Privacy Commissioner

6–1 Is the legislative structure pertaining to the Office of the Privacy Commissioner established under the *Privacy Act* appropriately meeting the needs of the community?

6–2 Are the constraints imposed in the *Privacy Act* on the exercise by the Privacy Commissioner of powers conferred by the Act appropriate?

6–3 Does the Privacy Advisory Committee perform a useful role and have appropriate powers and functions? Are the fields of expertise represented on the Privacy Advisory Committee appropriate? Does the Privacy Advisory Committee, and the fields of expertise of Privacy Advisory Committee members, need to be set out in the *Privacy Act*?

6–4 Is the scope of immunities conferred on: (a) the Privacy Commissioner and his or her delegates; (b) an adjudicator appointed under a privacy code and his or her delegates; and (c) other persons, appropriate?

6–5 Are the Privacy Commissioner's powers to oversee the *Privacy Act* appropriate and exercised effectively? For example, are the Commissioner's

powers: (a) to furnish advice; (b) to research and monitor developments in data processing and computer technology; (c) to promote understanding of the IPPs and of the objects of the IPPs and the NPPs; (d) to undertake education programs to promote individual privacy protection; (e) relating to tax file numbers; (f) arising under other Acts, appropriate and exercised effectively?

6–6 Should the *Privacy Act* require a privacy impact assessment to be prepared for: (a) all proposed Commonwealth legislation; (b) other proposed projects or developments of agencies; or (c) other proposed projects or developments of organisations?

6–7 If privacy impact assessments are required:

(a) who should be involved in preparing the assessments;

(b) who should be entitled to view the results of the assessments;

(c) who should bear the cost of the assessments; and

(d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

6–8 Is the Personal Information Digest published in a useful manner? If not, how might it be improved? Is the record itself useful?

6–9 What powers should the Privacy Commissioner have to audit agencies and organisations?

6–10 Should organisations and agencies be required to self-audit periodically to ensure and to demonstrate compliance with the *Privacy Act*?

6–11 Should all the Privacy Commissioner's functions be consolidated in the *Privacy Act?*

6–12 Are the procedures under the *Privacy Act* for making and pursuing a complaint, including a representative complaint, appropriate? Are the Privacy Commissioner's powers to make preliminary inquiries and investigate complaints appropriate and effective?

6–13 Is the obligation of the Privacy Commissioner to investigate a complaint about an act or practice that may interfere with the privacy of an individual appropriate, and is it administered effectively?

6–14 Is the power of the Privacy Commissioner to investigate an act or practice that may interfere with the privacy of an individual appropriate, and is it used effectively?

6–15 Are the Privacy Commissioner's powers relating to the conduct of investigations appropriate and exercised effectively? For example, are the Commissioner's powers regarding: (a) appearances before the Commissioner; (b) conferences; (c) obtaining information and documents; (d) examining witnesses; (e) entering premises to gather information; (f) discussion of complaints with a Minister or other designated person; and (g) reports, appropriate and exercised effectively?

6–16 Are the Privacy Commissioner's powers under the *Privacy Act* to make determinations appropriate and administered effectively?

6–17 Are the *Privacy Act* provisions for enforcing determinations adequate and administered effectively?

6–18 Are the Privacy Commissioner's powers under the *Privacy Act* to make public interest determinations, including temporary public interest determinations, appropriate and administered effectively?

6–19 Are the *Privacy Act* provisions for obtaining injunctions adequate and effective?

6–20 Are the *Privacy Act* provisions for approving privacy codes appropriate and effective? Are privacy codes an appropriate method of regulating and complying with the Act? Why have privacy codes been so little used? Should the Privacy Commissioner have the power, on his or her initiative, to develop and impose a binding code on organisations or agencies?

6–21 Is the current compliance model used in the *Privacy Act* appropriate and effective to achieve the Act's purposes? If not, is that because of its content, its administration, or some other reason?

6–22 Does the range of remedies available to enforce rights and obligations created by the *Privacy Act* require expansion? For example, should the available remedies include any or all of the following for particular breaches of the Act:

(a) administrative penalties;

(b) enforceable undertakings or other coercive orders;

(c) remedies in the nature of damages;

(d) infringement notices;

(e) civil penalties;

(f) criminal sanctions?

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation

7–1 Does the multi-layered regulation of personal information create any difficulties? For example, does the multi-layered regulation of personal information:

(a) cause an unjustified compliance burden;

(b) create problems for organisations that operate in more than one Australian state or territory;

(c) complicate the implementation of programs and services at a national level;

(d) raise any issues in relation to the existence of multiple privacy regulators in particular industry sectors and across the states and territories; or

(e) act as a barrier to the sharing of information between public sector agencies and private sector organisations?

7–2 Do any issues arise for organisations that provide contracted services involving personal information to Australian Government, state or territory agencies? For example:

(a) are privacy provisions in Australian Government, state or territory agency contracts contributing to inconsistency and fragmentation in privacy regulation;

(b) are the *Privacy Act* provisions relating to Commonwealth contractors appropriate and effective;

(c) do issues arise for Commonwealth contractors that are subject to the NPPs and the IPPs;

(d) do any issues arise for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies;

(e) is there a concern that organisations acting under a state or territory contract may not be required to adhere to the same privacy standards that are applicable to private sector organisations under the *Privacy Act*? If so, how should that concern be addressed?

7–3 How should personal information held on residential tenancy databases be regulated? For example, should it be regulated under the *Privacy Act*, by a binding code, or in some other way?

7–4 Does the inconsistent use of terms and definitions under federal legislation that regulates the handling of personal information create any difficulties? If so, what are some examples of the difficulties created?

7–5 Do 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? If so, how should the interaction between the *Privacy Act* and these provisions be clarified?

7–6 Does the interaction between the *Privacy Act* and other federal legislation that regulates the handling of personal information require clarification? In particular:

(a) does 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;

(b) should the *Privacy Act* provide for a process of consultation prior to granting access to information that includes personal information about a third party rather than rely on the process outlined in the *Freedom of Information Act 1982* (Cth);

(c) should the *Privacy Act* and the *Freedom of Information Act 1982* (Cth) be administered by the same body;

(d) should the *Privacy Act* apply to certain classes of records in the open access period for the purposes of the *Archives Act 1983* (Cth);

(e) should the exemption under the *Archives Act 1983* (Cth) relating to 'information relating to the personal affairs of any person' be amended to provide an exemption in relation to 'personal information' as defined in the *Privacy Act*;

(f) should the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth) be consolidated in one Act;

(g) should federal legislation relating to the handling of tax file numbers and data-matching be consolidated in one Act? If so, should they be consolidated in the *Privacy Act*;

(h) should data-matching programs that fall outside the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) be more formally regulated;

(i) is personal information collected pursuant to the *Census and Statistics Act 1905* (Cth) adequately protected;

(j) is it 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;

(k) does the *Commonwealth Electoral Act 1918* (Cth) provide adequate protection of personal information included on the electoral roll;

(l) does the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) adequately protect personal information?

7–7 Do 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, should the *Privacy Act,* rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by Australian Government agencies?

7–8 Are the provisions in Part VIII of the *Privacy Act* necessary? If so, are the provisions adequate and should they be contained in the *Privacy Act* or elsewhere?

7–9 Do privacy rules, privacy codes and privacy 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?

8. Health Services and Research

8–1 Does the regulation of health information require a different and separate set of privacy principles to those used to regulate other sensitive personal information?

8–2 Should s 3 of the *Privacy Act* be amended to state that the Act is intended to regulate the handling of health information in the private sector to the exclusion of state and territory legislation?

8–3 Is the draft *National Health Privacy Code* an effective way to achieve a nationally consistent and appropriate regime for the regulation of health information? If so, what is the most effective model for implementing the draft *National Health Privacy Code?* If not, what other model should be adopted to achieve a nationally consistent and appropriate regime for the regulation of health information?

8–4 If the draft *National Health Privacy Code* is not implemented nationally, should the Australian Government adopt the Code as a schedule to the *Privacy Act*?

8–5 Do electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or the draft *National Health Privacy Code*?

8–6 The *National Health Act 1953* (Cth) requires the Privacy Commissioner to issue guidelines in relation to the handling of personal information collected in connection with claims under the Medicare Benefits Program and the Pharmaceutical Benefits Program. Is this an appropriate and effective role for the Privacy Commissioner?

8–7 Are the definitions of: (a) 'health information'; and (b) 'health service' in the draft *National Health Privacy Code* appropriate and effective? Should the *Privacy Act* be amended to adopt these definitions?

8–8 Should the *Privacy Act* be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act?

8–9 Is guidance by the Office of the Privacy Commissioner to clarify that organisations can disclose health information for the management, funding and monitoring of a health service an appropriate and effective response to concerns in this area? If not, what is an appropriate and effective response?

8–10 Is there evidence that the regulation of personal health information impedes the provision of appropriate health services to individuals? If so, what

changes are necessary to facilitate the provision of appropriate health services?

8–11 Does the *Privacy Act* provide an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent? Does the draft *National Health Privacy Code* provide a more appropriate and effective framework for handling health information in these circumstances?

8–12 Are there any other issues relating to consent to deal with health information in the health services context that the ALRC should consider?

8–13 Should the *Privacy Act* be amended to allow health service providers to collect information about third parties without their consent in line with Public Interest Determinations 9 and 9A? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of such information than the current provisions of the *Privacy Act*?

8–14 Should the *Privacy Act* 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?

8–15 Should NPP 10 of the *Privacy Act* be amended to clarify when health information may be collected without consent? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of health information without consent?

8–16 Are there any other issues relating to the collection of health information that the ALRC should consider?

8–17 Is guidance by the Office of the Privacy Commissioner an appropriate and effective response to concerns that the phrases in NPP 2, 'primary purpose of collection' and 'directly related to the primary purpose', might impede the appropriate management of an individual's health? If not, what is an appropriate and effective response?

8–18 Does NHPP 2 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for the use and disclosure of health information than the current provisions of the *Privacy Act*?

8–19 Are there any other issues relating to the use and disclosure of health information that the ALRC should consider?

8–20 Is the exception in NPP 6.1(b) in relation to providing access to health information (that is, that access may be denied if it would pose a serious threat to the life or health of any person) appropriate and effective? Should the exception 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?

8–21 Do NHPP 6 and Part 5 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for access to health information than the current provisions of the *Privacy Act*?

8–22 Should the *Privacy Act* be amended to deal expressly with the situation in which a health service provider ceases to operate? Does NHPP 10 of the draft *National Health Privacy Code* provide an appropriate and effective framework to deal with this situation?

8–23 Are there any other issues the ALRC should consider in relation to access to health information?

8–24 Does NHPP 11 of the draft *National Health Privacy Code* provide a more appropriate and effective framework to deal with the transfer of health information from one health service provider to another than the current provisions of the *Privacy Act*?

8–25 Is the current public interest test in the *Privacy Act* and Section 95 and Section 95A Guidelines (that the public interest in promoting research substantially outweighs the public interest in maintaining the level of protection of health information provided by the Act) appropriate and effective? If not, what is an appropriate and effective test?

8–26 Should the term 'research' be defined for the purposes of the *Privacy Act*? If so, how should the term be defined?

8–27 Should the *Privacy Act* be amended to include definitions of 'identifiable', 're-identifiable' and 'non-identifiable' personal information?

8–28 Should the *Privacy Act* draw a distinction between 'identifiable' and 're-identifiable' health information in the context of health and medical research?

8–29 What provision should be made for the use of health information without consent in health and medical research?

8–30 Does NPP 2 provide an appropriate and effective framework for the use, without consent, of health information in health and medical research?

8–31 Are Human Research Ethics Committees 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?

8–32 Are the requirements imposed on Human Research Ethics Committees by the Section 95 and Section 95A Guidelines issued under the *Privacy Act* appropriate and effective?

8–33 Does the *Privacy Act* provide an appropriate and effective regime for: (a) the establishment of health data registers; and (b) the inclusion and linkage of health information in data registers?

9. Children, Young People and Adults with a Decision-Making Disability

9–1 Should the protection of personal information for children and young people be dealt with expressly in the *Privacy Act*? If so, how should the Act be amended? For example, are there privacy issues arising in the areas of:

- child welfare, juvenile justice or family law;
- disclosure of health information to parents;
- information held by schools and child care centres;
- online consumer information;
- taking and publishing photographs;
- broadcasting of identifying images and information; or
- identification of children and young people in court records.

9–2 Are there any other issues relating to the privacy protection of children and young people that are currently outside the scope of the *Privacy Act* that need to be addressed?

9–3 Is there a need to amend the *Privacy Act* to facilitate better the protection of the personal information of adults with a decision-making disability? If so, what amendments are required? Are there any non-legislative options that should be adopted in relation to adults with a decision-making disability?

10. Telecommunications Privacy

10–1 Do the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) provide adequate and effective protection for the use, disclosure and storage of personal information?

10–2 What issues, if any, are raised by the interaction between the *Privacy Act* and the following Acts:

- *Telecommunications Act 1997* (Cth);
- *Telecommunications (Interception and Access) Act 1979* (Cth);
- *Spam Act 2003* (Cth);
- *Do Not Call Register Act 2006* (Cth)?

Are there acts and practices regulated by these Acts that would be dealt with better under the *Privacy Act*?

10–3 What bodies (public or private) should be involved in the regulation of personal information in the telecommunications industry?

11. Developing Technology

11–1 What new technologies, or new uses of existing technologies, will, in the future, impact significantly on privacy? How can such technologies be accommodated in a regulatory framework?

11–2 Should the *Privacy Act* be extended to cover: (a) any acts or practices of individuals relating to their personal, family or household affairs; or (b) exempt agencies or organisations that use certain types of technology or collect certain types of personal information?

11–3 Is there a need to amend the *Privacy Act* in light of technological developments? If so, what amendments are required? For example:

(a) should there be any additional limits on the collection of personal information;

(b) should agencies or organisations be required to obtain consent before using certain technologies to collect personal information? If so, should it be possible to refuse consent without any adverse consequences;

(c) should biometric information be included in the definition of 'sensitive information'; and

(d) should agencies or organisations be required to advise individuals of any misuse, loss or unauthorised access, modification or disclosure of personal information?

11–4 Should the *Privacy Act* be technologically neutral?

11–5 What issues are raised by the publication in electronic form of publicly available records such as public records, court records and media reports? Does the *Privacy Act* need to be amended in response to these issues?

12. Unique Multi-Purpose Identifiers

12–1 Are the schemes that regulate Tax File Numbers appropriate and effective?

12–2 What unique multi-purpose identifiers are currently in use in Australia? What are the benefits and privacy concerns of using unique multi-purpose identifiers in transactions with agencies or organisations?

12–3 What role, if any, should the *Privacy Act* play in the regulation of unique multi-purpose identifiers?

13. Transborder Data Protection

13–1 Does NPP 9 provide adequate and appropriate protection for personal information transferred from Australia to a foreign country? Does the relationship between NPP 2 (disclosure of personal information) and NPP 9 (international transfer of personal information) need to be clarified?

13–2 Should the *Privacy Act* be amended to clarify that NPP 9 applies when personal information is transferred outside Australia to a related body corporate?

13–3 What role, if any, should the Office of the Privacy Commissioner play in identifying countries that have equivalent *Privacy Act* protection for personal information?

13–4 Should organisations be required to inform individuals that their personal information is to be transferred outside Australia? If so, what form should such notification take?

13–5 Is adequacy of the *Privacy Act* under the European Union Data Protection Directive: (a) necessary for the effective conduct of business with European Union members; and (b) desirable for the effective protection of personal information transferred into and out of Australia? If so, what measures are necessary to ensure the adequacy of Australia's privacy regime under the European Union Data Protection Directive?

13–6 Does the APEC Privacy Framework provide an appropriate model for the protection of personal information transferred between countries? Are other standards, such as the Asia-Pacific Charter, a more appropriate model?

1. Introduction to the Inquiry

Contents

Background

1.1 On 30 January 2006, the Attorney-General of Australia 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] The *Privacy Act* itself was partially the

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.

product of a seven year research effort by the ALRC, which culminated in 1983 with the three volume report, *Privacy* (ALRC 22).[2] 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),[3] and partially implemented into domestic law Australia's obligations under art 17 of the *International Covenant on Civil and Political Rights* (ICCPR).[4]

1.2 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)[5]—is worthy of particular note.

1.3 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.[6]

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 (APEC), has created pressure for the alignment of our privacy protection with key trading partners. These issues will be considered in detail during the course of the Inquiry.

ALRC 22

1.5 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

---

2 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

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 below, and in detail in Ch 4.

4 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).

5 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979).

6 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.

completed on access to census records.[7] In the privacy inquiry, two discussion papers were produced—in 1977 and 1980.[8] The final report, *Privacy* (ALRC 22), was tabled in Parliament in December 1983. Discussion of the issues is contained in Volume 1 and the ALRC's recommendations are contained in Volume 2. Volume 2 also includes draft legislation. Volume 3 contains various appendices.[9]

1.6 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.

1.7 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. However, the ALRC noted that the sub-categories 'are not necessarily mutually exclusive'.[10]

1.8 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',[11] 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'[12] were given legislative force;
- access to, and an ability to correct, credit information was provided for; and

---

7 Australian Law Reform Commission, *Privacy and the Census*, DP 8 (1978); Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).

8 Australian Law Reform Commission, *Privacy and Publication—Proposals for Protection*, DP 2 (1977); Australian Law Reform Commission, *Privacy and Intrusions*, DP 13 (1980).

9 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.

10 Ibid, [1093].

11 Ibid, xliii.

12 Ibid, xliii.

- rules governing the use, disclosure and security of some forms of personal information were implemented.

OECD Guidelines

1.9 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.[13] The 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.[14]

1.10 Eight basic principles of national application are set out in Part Two of the OECD Guidelines:[15]

> **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.
>
> **Use Limitation Principle**—Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 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.

---

13 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

14 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.

15 The full text of the OECD Guidelines can be found at <www.oecd.org>.

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.

The OECD Guidelines, and subsequent models to facilitate transborder data protection, are discussed in detail in Chapters 4 and 13.

1.11 The following discussion outlines the recommendations in ALRC 22 relating to intrusions, and significant developments in the intervening period. Except to the extent discussed below and in subsequent chapters, the ALRC regards intrusions as generally falling outside the Terms of Reference of the current Inquiry.

Intrusions—ALRC 22 and subsequent developments

1.12 In ALRC 22, the ALRC made recommendations to tighten the laws relating to police or other officials exercising powers of arrest, search and entry. Basic principles were developed by the ALRC, and provisions designed to implement these principles were included in the ALRC's draft Bill.[16] In addition to the draft provisions, the ALRC recommended that the Human Rights Commission[17] undertake a review of all existing Commonwealth and territory legislation conferring intrusive powers. Finally, the ALRC also made recommendations in relation to unsolicited communications and optical surveillance.[18]

16 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Appendix A.
17 As it then was; it is now the Human Rights and Equal Opportunity Commission (HREOC).
18 For a discussion of optical surveillance, see Ch 11.

Body cavity searches

1.13 The ALRC identified body cavity searches as an area of particular concern. At the time of the report, no federal legislation specifically regulated body cavity searches. The ALRC recommended a new regime to apply to body cavity searches by Commonwealth officers, including the Australian Federal Police (AFP). In particular, the recommendation was that:

- general authority to 'search the person of' should not extend to a body cavity search;[19]
- a body cavity search should only be conducted by a medical practitioner after receiving judicial authority for the search;[20]
- new procedures be established relating to the consent of the person to be searched.[21]

1.14 Commonwealth legislation now generally acknowledges four different types of personal searches: ordinary search, frisk search, strip search and internal search. Only the latter involves a body cavity search. In general, the greater the level of intrusiveness, the greater the amount of protection afforded the person who is to be searched.[22]

1.15 The only Commonwealth legislation that currently provides for internal searches is the *Customs Act 1901* (Cth). While provisions covering internal searches were enacted in the *Customs Amendment 1979* (Cth), the provisions were never proclaimed, as they did not provide adequate protection to suspects.[23] It was not until 1991, with the commencement of the *Customs (Detention and Search) Act 1990* (Cth), that the various levels of searches, together with appropriate protections, were established.[24]

1.16 Only a medical practitioner can conduct an internal search. Judicial authority is required where consent is not given to the search, or where the person is considered in need of protection—that is, a person under 18 years of age, or in a mental or physical condition (whether temporary or permanent) that makes the person incapable of managing his or her affairs.[25] The Act contains provisions relating to detention of the person while consent or judicial authority is sought.

---

19 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1110].
20 Ibid, [1110].
21 Ibid, [1112].
22 See N Hancock, *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002: Bills Digest No 128 2001–02* (2002) Parliament of Australia—Parliamentary Library, 24–27.
23 Commonwealth, *Parliamentary Debates*, House of Representatives, 16 May 1990, 670 (P Baldwin—Minister for Higher Education and Employment Services).
24 See *Customs Act 1901* (Cth) pt XII div IB subdivision C for current provisions relating to internal searches.
25 Ibid s 4.

Seizure of records

1.17 In the early 1980s, privacy problems associated with the seizure of personal records in Australia were confined largely to the seizure of health records. The AFP had guidelines, developed in consultation with the Australian Medical Association, for the seizure of such records. The same guidelines were applied to the seizure of other professional records.[26]

1.18 The ALRC recommended that the AFP and other government agencies develop an analogous procedure to the seizure of company records under the *Companies Act 1981* (Cth).[27] The ALRC also recommended that complaints should be able to be made to the Privacy Commissioner concerning the exercise of such powers.[28]

1.19 Many law enforcement and regulatory agencies now have powers to seize records. There has been a lack of consistent development of these powers, which is one of the areas under consideration by an Administrative Review Council project on the coercive investigative powers of federal government agencies, which commenced in 2003. The project, which is ongoing, involves an assessment of powers used to obtain information (whether through documents or through answers to questions) that do not require the agency to apply for a court order. The ALRC understands that a draft Report is currently in preparation.

Listening devices

1.20 In 1983, the *Customs Act* and the *Australian Security Intelligence Organisation Act 1979* (Cth) prohibited the use of listening devices, except in certain circumstances. Each Act sets out a detailed procedure for obtaining a judicial warrant to use a listening device.[29]

1.21 In ALRC 22, the ALRC recommended that Commonwealth legislation generally should prohibit the use of listening devices for non-consensual or secret surveillance. The ALRC concluded that 'it is inconsistent with personal privacy that listening devices be used to overhear or record conversations that are intended by their participants to be private'.[30] Two exceptions to this general prohibition were recommended.

1.22 First, consistent with prevailing international standards and overseas laws, a majority of the ALRC recommended that participant monitoring should not be

---

26 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1114].
27 Ibid, [1116].
28 Ibid, [1116].
29 Ibid, [1124].
30 Ibid, [1126].

prohibited.[31] 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.[32]

1.23 Secondly, the ALRC recommended that the AFP be allowed to use secret listening devices for law enforcement purposes after a judicial warrant was obtained. The warrant procedure in the *Customs Act* was considered a suitable model.[33]

1.24 In 1990, a procedure to obtain a warrant to use listening devices in relation to non-narcotic offences, similar to the procedure in the *Customs Act*, was introduced into the *Australian Federal Police Act 1979* (Cth).[34] Until that time there had been no prohibition at the federal level on the use of listening devices in non-narcotics offences.

1.25 The relevant provisions in the *Australian Federal Police Act* and the *Customs Act* subsequently were repealed by the *Surveillance Devices Act 2004* (Cth). The object of this Act was to introduce 'a modernised statutory regime covering the use of surveillance devices for the investigation of Commonwealth offences and state offences with a federal aspect'.[35] The *Surveillance Devices Act* contains no general prohibition on the use of surveillance devices, but instead regulates their use by law enforcement agencies. The term 'surveillance device' is much broader than 'listening device', and encapsulates a wider range of surveillance technology.

1.26 The *Surveillance Devices Act* is model legislation developed by the Standing Committee of Attorneys-General (SCAG) and Australasian Police Ministers Council Joint Working Group on National Investigative Powers.[36] While a warrant procedure continues to apply—and privacy is one of the issues that must be considered when deciding whether to grant a warrant—the Act differs from the ALRC 22 recommendations in a number of respects. The differences include:

- no general prohibition on the use of surveillance devices;
- in certain circumstances a surveillance device can be used without a warrant or authorisation. For example, optical surveillance devices can be used without a warrant if their use does not involve entry onto the premises under surveillance;

---

31 Ibid, [1127]–[1135]; however, note that two members of the ALRC dissented on this recommendation.
32 Ibid, [1127].
33 Ibid, [1124]. The use of listening devices by officers of the Australian Security Intelligence Organisation was excluded from the ALRC's Terms of Reference.
34 *Law and Justice Amendment Act 1989* (Cth).
35 J Norberry, *Surveillance Devices Bill 2004: Bills Digest No 147 2003–04* (2004) Parliament of Australia—Parliamentary Library, 1.
36 Standing Committee of Attorneys-General and Australasian Police Ministers Council Joint Working Group on National Investigative Powers, *Cross-Border Investigative Powers for Law Enforcement: Report* (2003).

- information obtained using a surveillance device is not always given protective status; and

- warrants can be obtained where the offence in question has a penalty of three years, rather than seven years[37] as recommended by the ALRC.[38]

1.27 The Act also provides that a listening device can be used without warrant where the officer is participating in the conversation.[39] This is consistent with the majority view expressed in ALRC 22 regarding participant monitoring.[40]

1.28 Use of surveillance devices by the Australian Security Intelligence Organisation (ASIO) continues to be regulated by the *Australian Security Intelligence Organisation Act*. Intelligence gathering functions of the Australian Security Intelligence Service and the Defence Signals Directorate are found in the *Intelligence Services Act 2001* (Cth). While a warrant procedure remains in place, the surveillance powers have extended beyond those considered in ALRC 22.

Telecommunications interception

1.29 In 1983, the interception of a telecommunication was governed by the *Telecommunications (Interception) Act 1979* (Cth). The Act prohibited interception, except in limited circumstances. Warrants could be granted under the Act in cases of national security or law enforcement in connection with narcotics offences.[41]

1.30 In ALRC 22, a number of recommendations called for reform of the *Telecommunications (Interception) Act*. For example, the ALRC recommended the removal of restrictions on participant monitoring,[42] and the extension of the Act to the interception of communications.[43] The ALRC did recommend an exception to the prohibition on the use of telecommunication interception for law enforcement purposes by the AFP. This recommended exception would be strictly controlled, and only would operate after a judicial warrant had been obtained.[44]

1.31 Interception of telecommunications continues to be governed by the *Telecommunications (Interception) Act*—the name of which was changed in 2006 to the *Telecommunications (Interception and Access) Act 1979* (Cth). There have been

---

37 As in the *Telecommunications (Interception) Act 1979* (Cth) s 7(6)(c).
38 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1164].
39 *Surveillance Devices Act 2004* (Cth) s 38.
40 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1133].
41 Ibid, [1138].
42 See Ibid, [1144].
43 Ibid, [1145].
44 Ibid, [1157], although many of the restrictions were already in place in the *Telecommunications (Interception) Act 1979* (Cth).

further amendments to the 1979 Act. In particular, the *Telecommunications (Interception) Amendment Act 2006* (Cth) introduced substantial reforms—such as the insertion of a warrant procedure to provide for law enforcement access to stored communications and access to emails.[45]

1.32 The *Telecommunications (Interception) Act* has never been amended to allow participant monitoring. In the Explanatory Memorandum to the Telecommunications (Interception) Amendment Bill 2006 (Cth), participant monitoring was seen as a breach of the 'strict privacy protections' contained within the Act.[46] The topic of telecommunications privacy is discussed in detail in Chapter 10.

Mail

1.33 In ALRC 22, the ALRC considered the privacy of the mail as fundamental to the protection of privacy. The ALRC made a number of recommendations aimed at ensuring the integrity of the postal system, and paid particular attention to the legality of regulations permitting Australia Post officials to open mail.[47]

1.34 In 1994, the statutory authority to open mail was moved from the *Postal Services Regulations* to the *Australian Postal Corporation Act 1989* (Cth).[48] The provisions include a general prohibition on opening mail, and then set out the circumstances in which postal officers or customs officers may open and examine mail. Of particular relevance to the current Inquiry, there are provisions that provide for disclosure of information in a range of circumstances, including for law enforcement purposes.[49]

Unsolicited communications

1.35 Direct marketing by mail and telephone, and telephone canvassing, were raised as issues of concern in ALRC 22. In relation to unsolicited personally addressed mail, the uncertainty surrounding the source from which contact details were obtained was raised as an issue.[50] On the issue of unsolicited telephone calls, the ALRC noted:

---

45 The 2006 Act implemented the Blunn Report: see A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department. The legislation was controversial. For example, see Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Telecommunications (Interception) Amendment Bill 2006* (2006), especially the Supplementary Report with Additional Comments of Dissent by the Australian Democrats; S Harris Rimmer, *Telecommunications (Interception) Amendment Bill 2006: Bills Digest No 102 2005–06* (2006) Parliament of Australia—Parliamentary Library.

46 Explanatory Memorandum, Telecommunications (Interception) Amendment Bill 2006 (Cth), 49 in discussion on repeal of s 6(2).

47 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1151]–[1154].

48 The *Australian Postal Corporation Amendment Act 1994* (Cth) inserted provisions relating to opening mail and disclosure of information by postal officers into the *Australian Postal Corporation Act 1989* (Cth) ss 90N, 90P–90T.

49 *Australian Postal Corporation Act 1989* (Cth) ss 90G–90LH.

50 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1177].

> Some people regard unwanted or unexpected telephone calls as especially intrusive. Unlike unsolicited mail, one cannot deal with an unwanted telephone call without paying some attention to it. Moreover, an unwanted call can be frightening or disturbing to vulnerable subscribers.[51]

1.36 The ALRC considered that the production of guidelines, developed by the Human Rights Commission in conjunction with industry representatives and consumer groups, would address the concerns. The ALRC also recommended that the Privacy Commissioner, through the complaints and conciliation function, monitor the guidelines.[52]

1.37 In 1998, the Australian Direct Marketing Association (ADMA), in conjunction with the Ministerial Council of Consumer Affairs and the Australian Competition and Consumer Commission, developed a code of practice relating to direct marketing. The code of practice is updated periodically.[53] Complaints can be made to the ADMA Code Authority. ADMA also has a 'Do Not Mail/Call' service for residential addresses and phone numbers, and codes of practice covering e-marketing and m-marketing (the use of SMS messages and other mobile wireless marketing technology).[54] In 2005, ADMA introduced guidelines for telephone marketing.[55]

1.38 Other measures to combat unsolicited communications include the *Spam Act 2003* (Cth). The Act prohibits the sending of unsolicited commercial electronic messages. The Act was developed in response to concerns that increasing volumes of spam could threaten the viability and efficiency of electronic messaging by damaging consumer confidence, obstructing legitimate business activity and imposing costs on users.[56]

1.39 The expansion of direct marketing services and consumer concerns, together with the existence of a variety of inconsistent Commonwealth, state and territory laws, prompted the Australian Government to establish a 'Do Not Call Register'.[57] The Australian Communications and Media Authority (ACMA) has responsibility for implementing the Register. The Register should be operational by early 2007.

---

51 Ibid, [1180]. Similar concerns were expressed by a number of respondents to the ALRC's National Privacy Phone-in, conducted on 1–2 June 2006. See Australian Law Reform Commission, 'Telemarketing, Information Privacy Top Community Concerns' (Press Release, 5 June 2006).

52 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1182].

53 The current version is Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2001).

54 Australian Direct Marketing Association, *Australian eMarketing Code of Practice* (2004); Australian Direct Marketing Association, *M-Marketing Code of Practice* (2003): see <www.adma.com.au>.

55 Australian Direct Marketing Association, *Telephone Marketing Guidelines* (2005): see <www.adma.com.au>.

56 National Office for the Information Economy, *Spam Act 2003: A Practical Guide for Business* (2004), 2.

57 *Do Not Call Register Act 2006* (Cth).

1.40 In this Inquiry, recent legislative initiatives to control unsolicited communications will be considered only to the extent that the legislation is inconsistent with the provisions of the *Privacy Act*, and the ALRC's ultimate recommendations for reform of that Act.

Privacy Act 1988 (Cth)

1.41 Initially, the *Privacy Act* applied exclusively to the Commonwealth public sector. Public sector agencies are required to comply with Information Privacy Principles (IPPs) that are similar, but not identical, to the OECD Guidelines. Dr Moira Paterson notes:

> It 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.[58]

1.42 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.[59] The IPPs and the NPPs are discussed in greater detail in Chapter 4. A general overview of the *Privacy Act* is provided in Chapter 3.

Privacy beyond the individual

Current scope of the Act

1.43 An important question arises as to who should be entitled to claim the protection of privacy legislation. Privacy law traditionally 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.[60] For ease of reference, the term 'group' is used here to refer to all such collective entities.

1.44 The *Privacy Act* explicitly confers protection on 'individuals'.[61] The Act defines 'individual' to mean 'a natural person'.[62] The omission of groups from the ambit of the Act was deliberate, reflecting the rejection of the notion of 'corporate privacy' in ALRC 22.[63] The ALRC justified this position by reference to the terms of art 17 of the

---

58 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [2.54].

59 *Privacy Amendment (Private Sector) Act 2000* (Cth) which came into effect on 21 December 2001.

60 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].

61 *Privacy Act 1988* (Cth) pt III, div 1.

62 Ibid s 6(1). 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).

63 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [27].

ICCPR,[64] the approach taken in most overseas privacy legislation and its Terms of Reference.[65] This also reflects the policy position of the OECD.[66]

1.45 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 especially to 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'.

Privacy and groups

1.46 There are three ways in which privacy protection can be made to 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*.

1.47 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 *Privacy 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 Local Medical Services Pty Ltd, be entitled to access to information about both his corporation and himself?[67]

1.48 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.[68]

---

64 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

65 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [27].

66 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [31]–[33].

67 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [29].

68 Ibid, [29].

1.49 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*. In considering reform, there are therefore two related questions about whether the *Privacy Act* should be amended to provide direct protection to groups, and if so, which groups should be covered by the Act.

Indigenous groups

1.50 It has been suggested that the *Privacy Act* be amended to respond better to the requirements of Indigenous groups—in particular, those groups' traditional laws and customs. There is some precedent for this at common law and in Northern Territory legislation.

1.51 Australian courts generally have responded to the need to maintain the confidentiality of certain information relating to the traditional laws and customs of Indigenous groups.[69] A good example is the case of *Maurice*, in which 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.[70] The 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 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.[71]

1.52 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 Federal Court of Australia agreed with this approach—that is, it accorded some limited protection to maintaining the privacy of this information, which was of particular importance to the Aboriginal group in question.[72]

1.53 There is some direct data protection for Indigenous groups in the *Information Act 2002* (NT). That Act contains a general requirement that government information be made publicly available, with an exemption where 'it is not in the public interest to

---

69 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].

70 *Aboriginal Sacred Sites Protection Authority v Maurice; Re the Warumungu Claim* (1986) 10 FCR 104.

71 Ibid, 107.

72 Ibid.

disclose the information'.[73] Section 56 then provides a specific 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.

1.54 It is also worth noting that the National Health and Medical Research Council (NHMRC) advises that those conducting medical research should not only consider the privacy concerns of individuals but also 'collectivities', which 'may include cultural or ethnic groups, and indigenous communities'.[74] For instance, the NHMRC states that it is necessary to address 'issues of consent, privacy, confidentiality and harms within the collectivity, to either individuals or the collectivity'.[75]

Corporations

1.55 It also has been suggested that the *Privacy Act* be extended to protect the privacy rights of corporations. Carolyn Doyle and Professor Mirko Bagaric argue that the right to privacy traditionally has been limited to natural persons because—in their view erroneously—privacy has been inextricably linked to autonomy and dignity.[76] Shorn of this link, they see no reason why the same privacy rights enjoyed by natural persons should not be extended to corporations.[77]

1.56 It should be noted that, if adopted, this would amount to a very significant extension of the *Privacy Act*. Moreover, it would constitute a departure from the policy approach adopted in the Act, and would require a fundamental re-conceptualisation of privacy. Privacy is, in law, generally considered a *human* right.[78] The status of the concept of privacy is discussed in greater detail below.

---

73 *Information Act 2002* (NT) s 50(1).

74 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), 31.

75 Ibid, 31.

76 C Doyle and M Bagaric, 'The Right to Privacy and Corporations' (2003) 31 *Australian Business Law Review* 237, 246–250.

77 Ibid, 250.

78 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: *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 326–327.

1.57 Without detracting from the universality of human rights, there is relatively broad acceptance for the proposition that a human right can attach to a group of people united by, for example, ethnic origin or religion.[79] 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.[80]

1.58 To take a hypothetical example: assuming there exists a universal right to health care, it would be pointless to insist that the right to health care means that men and women should be allocated identical gynaecological and obstetric services. The right to health care must instead mean 'the right to such health care as is necessary for the individual in question'. For this reason, if the *Privacy Act* were extended to protect the privacy rights of Indigenous or other ethnic groups, this would not necessarily cause friction with human rights law, provided that the extension constituted a rational response to the particular circumstances and privacy needs of those groups. Consequently, this would likely be seen as an incremental, as distinct from a radical, change.

1.59 Extending privacy law protection to entities involved in commerce would be a more drastic change. The problem is particularly acute in relation to corporations. Part of a corporation's *raison d'etre* is to create a barrier between the identity of the corporate entity and the identity of the persons who establish and run 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 require a re-conceptualisation of corporations law).

1.60 However, this problem might be less acute in relation to a commercial entity whose identity is less distinct from the individual or individuals who make up the entity. A partnership, for instance, more closely resembles in law a mere collection of people, rather than a distinct legal entity like a corporation.

---

79 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'.

80 See, eg, D Feldman, *Civil Liberties and Human Rights in England and Wales* (2nd ed, 2002), 13–14.

Question 1–1 Should the *Privacy Act* be amended to provide direct protection to groups such as: (a) Indigenous or other ethnic groups; or (b) commercial entities? If so, which groups or commercial entities should be covered by the Act?

The scope of the Inquiry

Terms of Reference

1.61 The Terms of Reference are reproduced at the beginning of this Issues 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.

1.62 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;
- 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.

1.63 The ALRC is directed to identify and consult with relevant stakeholders, including the Office of the Privacy Commissioner (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.

1.64 As noted above, 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. Information privacy is the primary focus, which includes information collection, access, use and disposal. Therefore, the scope of the current Inquiry is not as broad as ALRC 22. In particular, intrusions only will be reviewed if they fall within the scope of information collection, access or use. For example, how a marketer obtains a telephone number that results in an unsolicited telephone communication may fall within the scope of the Inquiry; the intrusion itself does not.

1.65 The ALRC also is directed to consider emerging areas that may require privacy protection. One such area is the emerging cause of action in Australia for breach of privacy. This is discussed in greater detail below.

The VLRC and NSWLRC privacy references

VLRC privacy reference

1.66 In March 2002, the Victorian Law Reform Commission (VLRC) was asked to examine two issues of public concern relating to privacy: workers' privacy and privacy in public places.[81] The first phase of this inquiry on workers' privacy has been completed,[82] and the VLRC has now embarked on its inquiry into surveillance in public places. The ALRC is liaising closely with the VLRC.

Workplace privacy

1.67 Apart from the issue of whether employee records should be exempt from the provisions of the *Privacy Act*,[83] the ALRC does not propose in this Inquiry to deal with the specific issue of workplace privacy. The ALRC has been advised that SCAG is currently considering the issue. This follows the recent completion by the VLRC of its inquiry into workplace privacy, which considered surveillance, monitoring, physical

---

81 Victorian Law Reform Commission, *Workplace Privacy: Options Paper* (2004), [1.1]. The Terms of Reference can be found at <www.lawreform.vic.gov.au>.

82 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).

83 The use and disclosure of workers' personal information is discussed in Ch 5.

and psychological testing, searching of workers and the collection, use and disclosure of workers' personal information.[84] The VLRC's final Report included a draft Workplace Privacy Bill.

NSWLRC privacy reference

1.68 On 11 April 2006, the New South Wales Law Reform Commission (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), the *Health Records and Information Privacy Protection Act 2002* (NSW), the *State Records Act 1998* (NSW), the *Freedom of Information Act 1989* (NSW) and the *Local Government Act 1993* (NSW);
- the desirability of introducing a statutory tort of privacy in New South Wales; and
- any related matters.

1.69 The NSWLRC is also directed to liaise with the ALRC and other relevant Commonwealth, state and territory agencies. While it is currently the intention of the ALRC and NSWLRC to produce separate consultation papers and final reports, the two Commissions will work together closely.

Protection of a right to personal privacy in Australia

Introduction

1.70 In referring to Australian actor, Heath Ledger, an Australian paparazzi photographer is reported to have said:

> It's the price of fame, my son. If we stop taking his picture, his price goes down. This is give-and-take. It's fame. It's the name of the game. You give us some of your private life because you earn so much money. That's the way it works.[85]

---

84 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).

85 G Bearup, 'Shooting Star', *Sydney Morning Herald Good Weekend* (Sydney), 1 July 2006, 26.

1.71 While the comments were made in the context of celebrity paparazzi photography, in law the comments would apply to anyone—celebrity, politician, person-of-interest in a criminal investigation, etc. Professor Des Butler notes that:

> Although legislation has been enacted at federal and state levels protecting the privacy of information and communications, it has long been asserted that the common law of Australia did not recognise an enforceable right to personal privacy.[86]

1.72 In ALRC 22, the ALRC rejected the creation of a general tort of invasion of privacy. In the ALRC's view at that time, '[s]uch a tort would be too vague and nebulous'.[87] In the intervening period there has been some movement in Australia and in other jurisdictions towards the recognition of an action for breach of privacy.

Australia

1.73 At common law, the major obstacle to the recognition in Australia of a right to privacy was, before 2001, the 1937 High Court of Australia decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* ('*Victoria Park*').[88] In a subsequent decision, the High Court in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* ('*Lenah 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]'.[89] 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.[90]

1.74 Only one Australian case has expressly recognised a common law right of action for a breach of an individual's right to 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.[91] After noting that the High Court in *Lenah Meats* had removed the barrier the *Victoria Park* case posed to any party attempting to rely on the tort of invasion of privacy, his Honour took what he viewed as 'a logical and desirable step'[92] and

---

86 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 339.

87 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1081].

88 *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, 341; Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [223].

89 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 248 (per Gummow and Hayne JJ, with whom Gaudron J agreed). See also Ibid at 277 (per Kirby J); 320–324 (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.

90 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.

91 *Grosse v Purvis* [2003] QDC 151.

92 Ibid, [442].

recognised 'a civil action for damages based on the actionable right of an individual person to privacy'.[93]

1.75 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.[94]

1.76 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.[95]

1.77 To date, no other Australian court has followed suit in recognising a cause of action for breach of privacy. In fact, the scant judicial commentary on the issue leans in the opposite direction.[96] In *Giller v Procopets*, Gillard J of the Supreme Court of Victoria noted that:

> Although it has been advocated from time to time that there should be a cause of action based on failure to respect the privacy of a person, both English and Australian law have not recognised a cause of action based upon breach of privacy.[97]

His Honour concluded that, 'in my opinion the law has not developed to the point where the law in Australia recognises an action for breach of privacy'.[98]

United States

1.78 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 [her] private affairs or concerns, is subject to liability

---

93 Ibid, [442].
94 Ibid, [444].
95 Ibid, [34].
96 See, eg, *Giller v Procopets* [2004] VSC 113; *Kalaba v Commonwealth* [2004] FCA 763; leave to appeal refused: *Kalaba v Commonwealth* [2004] FCAFC 326.
97 *Giller v Procopets* [2004] VSC 113, [187].
98 Ibid, [188]. For a critique of this judgment, see D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 361–363.

> to the other for invasion of his [her] privacy, if the intrusion would be highly offensive to a reasonable person;
>
> 2 One who appropriates to his [her] own use or benefit the name or likeness of another is subject to liability to the other for invasion of his [her] 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 [her] 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 [her] 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.[99]

1.79 The defences to the privacy torts are subject to the same defences that apply in the United States to defamation.[100] 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.[101]

Canada

1.80 Protection of an individual's privacy has received statutory protection in four provinces in Canada.[102] 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'.[103] 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 of public interest.[104]

1.81 While the *Canadian Charter of Rights and Freedoms 1982*[105] does not specifically guarantee a right to privacy, the Supreme Court of Canada has interpreted the right to be secure against unreasonable search and seizure contained in s 8 to

---

99 *Restatement of the Law, 2nd, Torts 1977* (US) §§ 652B, 652C, 652D, 652E.

100 Ibid, §§ 652F–652H.

101 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 343.

102 *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).

103 *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.

104 *Privacy Act 1978* RSS c P–24 (Saskatchewan) s 4. See also *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.

105 Enacted as Schedule B to the *Canada Act 1982* c 11 (UK), which came into force on 17 April 1982.

include a reasonable expectation of privacy in relation to governmental acts.[106] The province of Quebec has guaranteed 'a right to respect for his [her] personal life' in the Quebec *Charter of Human Rights and Freedoms*.[107]

New Zealand

1.82 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.[108] While the majority took pains to stress that 'the cause of action will evolve through future decisions as courts assess the nature and impact of particular circumstances',[109] 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[110] (noted above) 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.[111]

United Kingdom

1.83 In the United Kingdom, the cause of action for breach of confidence has been extended to encompass misuse or wrongful dissemination of private information.[112] Professor 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

106 *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').

107 *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].

108 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.

109 *Hosking v Runting* [2005] 1 NZLR 1, [118].

110 Ibid, [118]. The third formulation is outlined at [1.78] above.

111 Ibid, [117].

112 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].

> or ought to know that another person reasonably expects his or her privacy to be respected.[113]

1.84 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. The test for the 'privacy' of information, i.e. information that warrants protection (that its disclosure would be highly offensive to a reasonable person of ordinary sensibilities), taken in *Campbell* from the judgment of Gleeson CJ in the High Court of Australia in *Australian Broadcasting Corporation v Lenah Game Meats* comes directly from the American privacy jurisprudence.[114]

1.85 The European Convention on Human Rights[115] came into force in the United Kingdom in October 2000.[116] Since that time the courts in the United Kingdom have been influenced by art 8 of the Convention and by the Strasbourg jurisprudence interpreting art 8.[117]

Matters for the Inquiry

1.86 Should a cause of action for breach of privacy be recognised in Australia? If so, should the recognition of the cause of action be left to the courts or to the legislature? In *Lenah Meats*, Callinan J expressed a view on this issue.

> It seems to me that, having regard to current conditions in this country, and developments of the law in other common law jurisdictions, the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country, or whether the legislatures should be left to determine whether provisions for a remedy for it should be made.[118]

1.87 As noted above, the question falls squarely within the NSWLRC's Terms of Reference. The ALRC has agreed that the NSWLRC will take primary responsibility for the formulation of proposals for reform. With the consent of those consulted and making submissions to either review, consultation notes and submissions pertaining to this issue will be shared. However, the ALRC will revisit this area in the final report of this Inquiry.

---

113 D Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339, 350.

114 *Hosking v Runting* [2005] 1 NZLR 1, [43].

115 *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).

116 The Convention was implemented by the *Human Rights Act 1998* (UK).

117 See *McKennitt v Ash* [2005] EWHC 303 (QB), [49].

118 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, [335].

Question 1–2 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?

Defining 'privacy'

1.88 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.[119]

1.89 As the preceding discussion illustrates, the issues to be covered in this Inquiry do not fall neatly into one concept; however, the primary focus will be on information privacy.

1.90 The recognition of a general right to privacy warranting legal protection is a relatively modern phenomenon.[120] While the genesis of modern legal academic discussion of the topic is generally acknowledged to be Samuel Warren and Louis Brandeis's article, 'The Right to Privacy' published in the *Harvard Law Review* in

---

119 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 1 September 2006.

120 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 465.

1890,[121] widespread debate, particularly in the United States, can be traced to the 1960s[122] and subsequent decades.[123]

1.91 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.[124]

1.92 Other factors, according to Professor Gavison, include the advent of tabloid journalism, and the 'tendency to put old claims in new terms'.[125]

1.93 The ALRC indicated in ALRC 22 that the chief threats to privacy in Australia include:

> *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.[126]

1.94 All of these factors, as evidenced by the Terms of Reference for this Inquiry, resonate with equal, if not greater, force today.

1.95 Why is privacy considered important? What is the nature of the legal 'right' requiring protection? In answer to the first question, Professor Roger Clarke suggests

---

121 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

122 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 1960. 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.

123 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 *Metphilosophy* 259; D Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087.

124 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.

125 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 466.

126 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), xli.

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. …
>
> **Economicall**y, 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.[127]

1.96 The answer to the second question is more difficult. Despite the best efforts of legal scholars, the term 'privacy' eludes a universally accepted definition.[128] In ALRC 22 it was noted that 'the very term "privacy" is one fraught with difficulty. The concept is an elusive one.'[129] As Professor J Thomas McCarthy notes:

> 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.[130]

1.97 In ALRC 22, the ALRC adopted a definition of the term 'privacy' that 'stayed as close as possible … to the ordinary language concept'.[131] This approach has been criticised. Senator Brett Mason suggests that, in this regard, 'the Commission's *Report* is stronger on the practical application of legal rules and remedies to certain privacy issues than it is on theoretical analysis'.[132] He concludes that 'the ordinary language concept of "privacy" … does not necessarily inform a sensible legal right'.[133]

1.98 Senator Mason, like Professor McCarthy, goes on to argue that 'privacy' 'has no core that survives normative analysis'.[134] According to Senator 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

---

127 R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 7 August 2006.

128 L Introna, 'Privacy and the Computer: Why We Need Privacy in the Information Society' (1997) 28 *Metphilosophy* 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.

129 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [19].

130 J McCarthy, *The Rights of Publicity and Privacy* (2nd ed, 2005), [5.59]. See also D Solove, 'A Taxonomy of Privacy' (2006) *University of Pennsylvania Law Review* 477, 479.

131 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [20].

132 B Mason, *Privacy Without Principle* (2006), 40.

133 Ibid, 41.

134 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.[135]

1.99 Professor James Whitman suggests that 'there is no such thing as privacy as such'.[136] Comparing American, French and German approaches to privacy, Professor 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.[137]

1.100 Professor 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'.[138] By contrast, the conceptual core of the American right to privacy is, according to Professor Whitman, the 'right to freedom from intrusions by the state, especially in one's own home'.[139]

1.101 Professor Whitman emphasises that the differences between American and European privacy law are comparative, not absolute.[140] 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'.[141] However, the differences are real.

1.102 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 beginning to emerge as a topic in Asia. What works in one country or region doesn't always work in the other.[142]

---

135 Ibid, 80.

136 J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 1151, 1221.

137 Ibid, 1163. See also, R Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 569.

138 J Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 1151, 1161.

139 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.

140 Ibid, 1203.

141 Ibid, 1219.

142 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.

1.103 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, it has been 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'.[143]

1.104 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.[144]

Towards a working definition

1.105 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*,[145] and the ICCPR.[146] 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',[147] the recognition of privacy as a human right in the ICCPR lends support to the argument that such recognition in domestic law is warranted.

1.106 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; …

---

143 M Jackson, *Hughes on Data Protection in Australia* (2nd ed, 2001), 6.

144 The workshop participants included Professor Des Butler; Professor Roger Clarke; Professor David Kinley; Mr David Lindsay; Associate Professor Megan Richardson; and Dr Greg Taylor.

145 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).

146 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976) art 17.

147 *Dietrich v The Queen* (1992) 177 CLR 292, 305.

1.107 The *Human Rights Act 2004* (ACT) contains an almost identical provision.[148] 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.[149]

1.108 Professor Gavison suggests that 'privacy' is 'a term used with many meanings',[150] 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.[151]

1.109 Dealing first with the *status* of the term 'privacy' in an Australian context, the VLRC's *Workplace Privacy Issues Paper* proposes 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'.[152] The VLRC formulates 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'.[153]

1.110 Privacy also may be viewed as the bundle of interests that individuals have in the personal sphere free from interference from others.[154] In this formulation, the use of the term 'interest' rather than 'right' is intentional. This is not to suggest that privacy is not a 'right' in a legal sense; however, 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 rights in the legal sense.

1.111 Other theorists, such as Professor Daniel Solove, suggest that attempts to identify the essence of privacy—that is, the common denominator(s) that make things private—is misguided. Professor Solove argues that:

---

148 *Human Rights Act 2004* (ACT) s 12.

149 R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 7 August 2006.

150 R Gavison, 'Privacy and the Limits of Law' (1980) 89 *Yale Law Journal* 421, 424.

151 Ibid, 424.

152 Victorian Law Reform Commission, *Workplace Privacy: Issues Paper* (2002), xii. (Emphasis in text)

153 Ibid, [2.38]. Based on this working definition, the VLRC suggests 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].

154 See eg R Clarke, *What's 'Privacy'?* (2004) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html> at 7 August 2006.

> 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.[155]

1.112 Professor 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.[156]

1.113 However, some critics 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.[157]

1.114 The concept of privacy may also have a changing demographic dimension. For example, what baby boomers see as necessarily falling within the 'topography of the web' may not resonate with the internet generation. Young people appear much more willing to share personal details, post images and interact with others on internet chat sites.[158] Does this indicate a changing attitude to privacy? This issue will be explored in greater detail during the course of the Inquiry.

1.115 While it is important to recognise that the pragmatic approach advocated by theorists such as Professor Solove has limitations, it does provide 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, perhaps it makes more sense, to use Professor Solove's terms, to focus on particular points in the web and formulate a workable approach to deal with the disruption.[159] 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.

1.116 When undertaking this analysis it is important to bear in mind that privacy interests unavoidably will compete, collide and coexist with other interests. For

---

155 D Solove, 'Conceptualizing Privacy' (2002) 90 *California Law Review* 1087, 1099.
156 Ibid, 1130.
157 R Bruyer, 'Privacy: A Review and Critique of the Literature' (2006) 43 *Alberta Law Review* 553, 576.
158 L Weeks, 'See Me, Click Me: Your Life Is an Open Blog, Your Wit Updated 24/7. Still, Not Everyone is LOL', *Washington Post* (online), 23 July 2006, <www.washingtonpost.com>.
159 D Solove, 'A Taxonomy of Privacy' (2006) *University of Pennsylvania Law Review* 477, 485–486.

example, privacy often competes with freedom of the press, 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.[160]

1.117 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.[161]

1.118 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. … [E]ven 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.[162]

1.119 Ascertaining the appropriate policy to deal with the tension between competing interests is the challenge facing judges, legislators and law reformers. If equal protection is assured, however, it follows from the above discussion of the status accorded to privacy in international and domestic human rights instruments that privacy will take precedence over more basic interests, such as economic choice and opportunity.[163]

Organisation of this paper

1.120 This Issues Paper is organised into 13 chapters. Chapter 2 provides an overview of privacy regulation in Australia. It looks at how the *Australian Constitution* impacts on privacy regulation, and then considers the regulation of information privacy in the states and territories. Possible methods to achieve national consistency in the regulation of personal information are also discussed.

1.121 Chapter 3 focuses specifically on the *Privacy Act* and contains an overview of the Act in its current form. Basic issues in relation to the Act are raised, including whether the:

---

160 C Fried, 'Privacy' (1967) 77 *Yale Law Journal* 475, 478. See also *Privacy Act 1988* (Cth) s 29(a).

161 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

162 *McKennitt v Ash* [2005] EWHC 303 (QB), [57].

163 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.

- name of Act is accurate and appropriate;
- Act should include an objects clause;
- definitions in the Act are adequate and appropriate; and
- Act needs to be redrafted to achieve a greater degree of simplicity and clarity.

1.122 Chapter 4 examines the privacy principles in the *Privacy Act* that apply to public sector agencies (IPPs) and private sector organisations (NPPs). Whether there should be a single set of privacy principles is discussed, and privacy principles in other comparable jurisdictions are examined.

1.123 The application of the *Privacy Act* is limited by a number of exemptions and exceptions. Chapter 5 considers the role of exemptions, examines specific exemptions from the Act in the public and private sectors and canvasses the possibility of new exemptions.[164]

1.124 Chapter 6 discusses two key elements in effective privacy protection. The first is the OPC, which is the statutory body established under the *Privacy Act*. The second concerns the procedures established by the *Privacy Act* for monitoring and securing compliance with the Act. Both elements are considered, and issues are raised about the effectiveness of the current statutory regime for ensuring compliance with the Act.

1.125 Chapter 7 considers how the *Privacy Act* interacts with other federal, state and territory laws. Areas of fragmentation and inconsistency in the regulation of personal information are identified and discussed.

1.126 Chapter 8 focuses specifically on privacy issues relating to health services and medical research. While this Issues Paper is primarily concerned with privacy regulation, other ethical and legal duties imposed on health service providers will be considered in the context of the need for greater national consistency. State and territory health privacy legislation and the draft *National Health Privacy Code* are also considered.

1.127 Chapter 9 considers existing laws and practices applying to privacy of children and young people. The recognition at international law of the right of children to privacy—and how the *Privacy Act* and other Australian legislation impacts on the privacy of children and young people—are also addressed. The chapter also looks at adults with a decision-making disability and discusses whether there is a need to

164 Exceptions are discussed in Ch 4.

change the *Privacy Act* or other legislation to facilitate better the protection of the personal information of this group.

1.128 Chapter 10 outlines the different schemes that regulate the handling of personal information in the telecommunications context and examines the way in which these schemes interact with the *Privacy Act*. It also discusses legislation that has been introduced to control particular activities in the telecommunications context that impact on privacy, such as telemarketing.

1.129 Chapter 11 examines developing technology and privacy. It provides an overview of some of the developing technologies that have the potential both to erode and enhance privacy (such as biometrics and smartcards), and considers whether the existing means of regulating the use of such technologies is adequate and appropriate.

1.130 Chapter 12 discusses unique identifiers assigned to individuals by governments for use by multiple government agencies and organisations (unique multi-purpose identifiers). The chapter commences with an overview of concerns about the impact unique multi-purpose identifiers have on privacy. It then examines the history of identification schemes in Australia, including the Australia Card debate in the 1980s and the current debate surrounding the Australian Government's proposed Access Card. Finally, it considers identification schemes using multi-purpose identifiers in other countries.

1.131 Chapter 13 looks at transborder data protection. The chapter considers the extraterritorial operation of the *Privacy Act* and the restrictions on the transfer of information to countries with differing privacy regimes. The chapter then examines the two major international regimes aimed at harmonising information privacy protection principles—the APEC Privacy Framework[165] and the European Union Data Protection Directive[166]—and discusses whether Australia should amend its privacy regime to ensure compliance with those models.

Process of reform

Advisory Committee

1.132 It is standard operating procedure for the ALRC to establish an expert Advisory Committee to assist with the development of its inquiries.[167] In this Inquiry, the Advisory Committee includes current and former Privacy Commissioners; privacy and consumer advocates; privacy professionals; health and social service professionals; academics with expertise in privacy, health law and e-commerce; and public and private sector officers with responsibility for privacy.

---

165 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

166 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).

167 A list of Advisory Committee members can be found in the List of Participants at the front of this publication.

1.133 Given the breadth of this Inquiry, the ALRC also has established three sub-committees of the Advisory Committee in the areas of health privacy, technology and credit reporting. The health privacy sub-committee has been constituted,[168] and the technology and credit reporting sub-committees will be formed following the release of this Issues Paper.

1.134 The Advisory Committee met for the first time on 17 August 2006, and will meet at least two more times during the course of the Inquiry. The Advisory Committee has 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 also will assist with the development of reform proposals as the Inquiry progresses. However, the ultimate responsibility for the final Report and recommendations remains with the Commissioners of the ALRC.

Community consultation and participation

1.135 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.[169] One of the most important features of ALRC inquiries is the commitment to widespread community consultation.

1.136 The nature and extent of this engagement is normally determined by the subject matter of the reference. Areas that are seen to be narrow and technical tend to be of interest mainly to experts. Some ALRC references—such as those relating to children and the law, Aboriginal customary law, multiculturalism and the law, and the protection of human genetic information—involve a significant level of interest and involvement from the general public and the media. This Inquiry falls into the latter category and interest has been expressed by a wide cross-section of individuals, groups and organisations.

1.137 To date, consultations have been held with: privacy advocates; academics and lawyers with expertise in privacy; Australian Government departments, such as the Department of Foreign Affairs and Trade, and the Department of Communications, Technology and the Arts; state bodies such as the New South Wales Commission for Children and Young People, and the Victorian Government Office of the Health Services Commissioner; federal, state and territory privacy commissioners; business and consumer representatives; the Access Card Taskforce; and the NHMRC. In addition, the ALRC has made numerous presentations to a wide variety of interested groups.

---

168 A list of Health Privacy Sub-committee members can be found in the List of Participants at the front of this publication.

169 *Australian Law Reform Commission Act 1996* (Cth) s 38.

ALRC National Privacy Phone-in

1.138 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.

1.139 The majority of respondents (73%) nominated telemarketing as their main concern.[170] Other prominent issues included:[171]

- 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%).

1.140 The fact that callers could remain anonymous facilitated frank disclosure. The views expressed include 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.

Participating in the Inquiry

1.141 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 will receive notices, press releases and a copy of each consultation document produced during the Inquiry.

1.142 Secondly, individuals and organisations may make written submissions to the Inquiry, both after the release of the Issues Papers and again after the release of the 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 Issues Paper.

1.143 The ALRC strongly urges interested parties, and especially key stakeholders, to make submissions *before* the publication of the Discussion Paper. Once the basic

---

170 This was possibly influenced by the fact that a number of media stories about the Phone-in focused on telemarketing as a possible concern.

171 Callers were able to nominate more than one concern, which is reflected in the statistics.

pattern of proposals is established it is difficult for the ALRC to alter course radically. Although it is possible for the ALRC to abandon or substantially modify proposals for which there has been little support, it is more difficult to publicise, and gauge support for, novel approaches suggested to us late in the consultation process.

1.144 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.

1.145 Finally, in this Inquiry it is the intention of the ALRC to hold public meetings, and a series of roundtable discussions with specific interest groups such as small and large businesses, non-governmental organisations, consumer groups and so on.

Timeframe for the Inquiry

1.146 Two Issues Papers will be released during the course of this Inquiry. This Issues Paper deals with all matters relevant to the Terms of Reference, with the exception of the consumer credit reporting provisions. Issues Paper 32, which will deal with the consumer credit reporting provisions, will be released in December 2006.

1.147 The Issues Papers will be followed by the publication of a Discussion Paper in mid-2007. The Discussion Paper will contain a more detailed treatment of the issues, and will indicate the ALRC's current thinking in the form of specific reform proposals. The ALRC will then seek further submissions and undertake a further round of national consultations concerning these proposals. The Issues Papers and the Discussion Paper may be obtained from the ALRC free of charge in hard copy or on CD-ROM, and may be downloaded free of charge from the ALRC's website, <www.alrc.gov.au>.

1.148 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.[172] 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.[173]

---

172 The Attorney-General must table the Report within 15 sitting days of receiving it: *Australian Law Reform Commission Act 1996* (Cth) s 23.

173 However, 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.

1.149 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 Discussion Paper, **submissions addressing the questions in this Issues Paper must reach the ALRC by 15 January 2007**. Details about how to make a submission are set out at the front of this publication.

2. Overview of Privacy Regulation in Australia

Contents

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 following section outlines the regulation of privacy by the states and territories, and privacy rules, codes and guidelines. The final section considers various methods to achieve greater national consistency of Australian privacy laws.

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 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* (the 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]

2.5 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.

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 the Australian Capital Territory, of the Northern Territory and of Norfolk Island';[8]

---

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 1.
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 Chs 1 and 4.
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).
8 *Privacy Act 1988* (Cth) s 4.

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]

2.7 Section 6F of the *Privacy Act* allows the Act to be extended to cover the handling of personal information by state and territory authorities at the initiative of the states and territories. It would also be possible to amend the Act at the federal level to bring state and territory authorities within the definition of 'agency', subject to certain express and implied constitutional limitations.

2.8 Express constitutional limitations include those in ss 51(xiii) and 51(xiv) of the *Australian Constitution*, which provide that the Australian 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. This limitation is reflected in s 12A of the *Privacy Act*.[12]

2.9 Implied constitutional limitations include the principles that a federal law may not discriminate against a state,[13] or prevent a state from continuing to exist and function as an independent unit of the federation.[14] It is unlikely that a federal law relating to the handling of personal information by state public sector authorities would infringe these implied constitutional limitations. The Australian Parliament has plenary power to legislate in relation to the territories and so these same issues do not arise.[15] A range 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.

2.10 Section 3 of the *Privacy Amendment (Private Sector) Act* states that one of the main objects of the Act is

---

9 Ibid 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 5. 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).

12 *Privacy Act 1988* (Cth) s 12A.

13 *Victoria v Commonwealth* (1957) 99 CLR 575; *Western Australia v Commonwealth* (1995) 183 CLR 373.

14 *Victoria v Commonwealth* (1971) 122 CLR 353; *Re Australian Education Union; Ex parte Victoria* (1995) 184 CLR 188.

15 *Australian Constitution* s 122.

> 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.[16]

2.11 It does not appear, however, that the Act has achieved its goal. As discussed below, 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. The issues and problems inherent in this situation are discussed further in Chapters 7 and 8.

Saving of state and territory law

2.12 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;[17] 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.[18]

2.13 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.

2.14 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* does not, however, sit entirely comfortably with s 3 of the *Privacy Amendment (Private Sector) Act*.

2.15 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96) the ALRC and the Australian Health Ethics Committee (AHEC) considered whether the NSW, Victorian and ACT health privacy legislation might be inconsistent with the *Privacy Act* and to that extent invalid.[19] 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

---

16 *Privacy Amendment (Private Sector) Act 2000* (Cth) s 3(a).

17 *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.

18 *Clyde Engineering Co Ltd v Cowburn* (1926) 37 CLR 466.

19 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

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 that provides for more stringent genetic privacy protection'.[20]

2.16 The Office of the Privacy Commissioner 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.[21]

2.17 Any attempt by the Commonwealth to 'cover the field' in this way would, however, raise complex political and constitutional issues. In addition, this approach would not address other issues—such as complexity, fragmentation and inconsistency in privacy regulation across the public and private sectors. The following sections provide an overview of the regulatory regime in Australia and then consider various models—including national legislation and cooperative legislative schemes—for achieving greater consistency in this area.

Federal regulation of privacy

Privacy Act 1988 (Cth)

2.18 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*.

Other relevant federal legislation

2.19 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 regime if its disclosure would involve unreasonable disclosure of 'personal information'.[22] 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.[23] The *Archives Act 1983* (Cth) provides a similar exemption.[24]

---

20 Ibid, [7.44]–[7.49].

21 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.

22 *Freedom of Information Act 1982* (Cth) s 41.

23 Ibid s 41(2).

24 *Archives Act 1983* (Cth) s 33. See discussion in Ch 7.

2.20 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.

2.21 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) 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 Chapter 7.

State and territory regulation of privacy

2.22 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)

2.23 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).[25]

2.24 A number of the Information Privacy Principles are similar to the IPPs in the *Privacy Act*, but they are not identical.[26] There are four major sources of exemptions to the *Privacy and Personal Information Protection Act*: exemptions in the Act;[27] exemptions in regulations;[28] exemptions in a privacy code of practice, made by the

---

25 *Privacy and Personal Information Protection Act 1998* (NSW) s 4A. See the discussion of the *Health Records and Information Privacy Act 2002* (NSW) below.

26 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*.

27 For example, there are exemptions for law enforcement and investigative agencies: *Privacy and Personal Information Protection Act 1998* (NSW) pt 2 div 3.

28 For example, there are exemptions relating to privacy management plans under the *Privacy and Personal Information Protection Regulation 2005* (NSW) regs 5–7.

Attorney General;[29] and exemptions in a public interest direction made by the NSW Privacy Commissioner.[30]

2.25 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[31] 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.[32] The Act also provides for privacy management plans.[33]

2.26 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[34] and may also make written reports on any findings or recommendations made in relation to a complaint.[35] In 2004–05, Privacy NSW received 111 new complaints. The majority of those complaints were against state government agencies. However, a significant proportion were also against private organisations and local governments.[36] The most common complaints received by Privacy NSW were about disclosure, use, and access to information.[37]

Health Records and Information Privacy Act 2002 (NSW)

2.27 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*).[38] 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.[39]

2.28 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

29 *Privacy and Personal Information Protection Act 1998* (NSW) ss 29–32.
30 Ibid s 41.
31 Ibid s 30(1).
32 Ibid s 30(2).
33 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.
34 Ibid s 49.
35 Ibid s 50.
36 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.
37 Privacy NSW, *Annual Report 2004–05* (2005), 29.
38 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.
39 *Health Records and Information Privacy Act 2002* (NSW) s 3.

and anonymity, and transferrals and linkage.[40] The Act provides for a number of 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.[41] Further the HPPs themselves include exemptions.[42] Some of these exemptions are the subject of statutory guidelines.[43]

2.29 The NSW Privacy Commissioner has a number of functions under the Act, including functions relating to the receipt, investigation and conciliation of complaints about alleged contraventions of the HPPs.[44] In 2004–05, Privacy NSW received 28 complaints relating to health records.[45]

Other legislation

2.30 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.[46]

Victoria

Information Privacy Act 2000 (Vic)

2.31 The *Information Privacy Act 2000* (Vic) came into effect 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.[47] Organisations performing work for the Victorian government may also be subject to the Act, depending on the particular contract.[48]

---

40 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* was a particular issue: New South Wales, *Parliamentary Debates*, Legislative Council, 11 June 2002, 2958 (M Egan—Treasurer and Minister for State Development).

41 *Health Records and Information Privacy Act 2002* (NSW) s 17.

42 See, eg, Ibid sch 1, HPP 10(1)(c).

43 See, eg, Privacy NSW, *Health Records and Information Privacy Act 2002 (NSW): Statutory Guidelines on the Management of Health Services* (2004).

44 *Health Records and Information Privacy Act 2002* (NSW) s 58.

45 Privacy NSW, *Annual Report 2004–05* (2005), 29.

46 *Workplace Surveillance Act 2005* (NSW) pt 3.

47 *Information Privacy Act 2000* (Vic) s 9.

48 Ibid s 17.

2.32 The Act requires public sector agencies to comply with 10 Information Privacy Principles or have an approved code of practice.[49] The Information Privacy Principles are similar to the NPPs in the *Privacy Act*.[50] The Act contains a number of exemptions, including exemptions in relation to courts and tribunal proceedings, publicly available information and law enforcement.[51]

2.33 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.[52] 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.[53] The Office of the Victorian Privacy Commissioner received 50 new complaints in 2004–05. Seventeen of these were against local councils, 14 were against state government departments, nine were against statutory authorities and three against territory institutions. The remaining complaints were against various other public sector organisations. The most common complaints related to use and disclosure, data security and the collection of information.[54]

Health Records Act 2001 (Vic)

2.34 The *Health Records Act 2001* (Vic) covers the handling of all health information held by health service providers in the state public sector[55] and the private health sector.[56]

2.35 The Act contains 11 Health Privacy Principles adapted from the NPPs in the *Privacy Act*.[57] The Act contains a few exemptions to these principles, including

---

49 Codes of Practice are provided for in Ibid pt 4.

50 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.

51 *Information Privacy Act 2000* (Vic) pt 2 div 2.

52 Ibid s 58.

53 Ibid s 44.

54 Office of the Victorian Privacy Commissioner, *Annual Report 2004–05* (2005), 20–21.

55 *Health Records Act 2001* (Vic) s 10.

56 Ibid s 11.

57 '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.[58]

2.36 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.[59] 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.[60] The Office of the Health Services Commissioner closed 269 complaints under the Act in 2004–05. The most common complaints related to access and correction, use and disclosure and data quality.[61]

2.37 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.[62]

VLRC Review

2.38 In October 2005, the Victorian Law Reform Commission (VLRC) released *Workplace Privacy—Final Report* (2005).[63] 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.[64]

2.39 The Victorian Parliament has recently enacted the *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).[65] 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.[66] 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 of a worker in workplace toilets, washrooms, change rooms or lactation rooms.[67] There are some limited exceptions to this general prohibition.[68]

---

58 *Health Records Act 2001* (Vic) pt 2 div 3.
59 Ibid s 45.
60 Ibid pt 6.
61 Victorian Government Office of the Health Services Commissioner, *2005 Annual Report* (2005), 14.
62 *Health Records Act 2001* (Vic) pt 4.
63 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005).
64 Ibid, Recs 1–65.
65 The Act will commence on 1 July 2007: *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 2.
66 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), Rec 31.
67 *Surveillance Devices (Workplace Privacy) Act 2006* (Vic) s 3.
68 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.

Charter of Human Rights and Responsibilities Act 2006 (Vic)

2.40 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.[69] 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

2.41 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.[70] 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).[71]

Information Standard 42

2.42 *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*.

2.43 The Information Standard applies to all accountable officers and statutory bodies as defined under the *Financial Administration and Audit Act 1977* (Qld) (including government departments). It also applies to most statutory government owned corporations.[72] 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

---

69 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.

70 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].

71 *Financial Management Standard 1997* (Qld) ss 22(2) and 56(1).

72 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].

Information Standard; and compliance is subject to any existing outsourcing arrangements, contracts and licenses.[73]

2.44 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.[74]

2.45 The Information Standard contains a number of mandatory 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.[75] The Information Standard provides that agencies may develop codes of practice that modify the application of the Information Privacy Principles.[76] A set of guidelines has been developed to assist agencies to comply with their obligations under the Information Standard.[77]

Information Standard 42A

2.46 *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*.[78] 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).

2.47 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.[79]

Queensland Health Rights Commission

2.48 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 2004–05 it received 225 complaints related to 'privacy/discrimination' out of a total of 4163 complaints.[80]

---

73 Ibid, [1.1].
74 Ibid, [1.2].
75 Ibid, [3.1].
76 Ibid, [1.3].
77 Queensland Government, *Information Standard 42—Information Privacy Guidelines* (2001).
78 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001).
79 Queensland Government, *Information Standard 42A—Information Privacy Guidelines* (2001).
80 Queensland Goverment Health Rights Commission, *Annual Report 2004–2005* (2005), 10, 14.

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.

Other legislation

2.49 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

2.50 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.[81]

2.51 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.

2.52 In May 2003, the Western Australian Attorney-General, the Hon Jim McGinty MP, released a discussion paper proposing the introduction of Western Australian privacy laws. The proposed legislation would apply to the Western Australian public sector and private contractors working for government. It would apply to the private sector in relation to health information only. The discussion paper proposed a set of laws governing the collection, storage, release and use of personal information; and an independent Office of Privacy and Information Commissioner to administer the new laws, the *Freedom of Information Act 1992* (WA) and to oversee enforcement.[83] To date, a final report has not been released.

---

81 *Freedom of Information Act 1992* (WA) Glossary.

82 *State Records Act 2000* (WA) s 49.

83 See Office of the Attorney General for Western Australia, *Privacy Legislation for Western Australia Discussion Paper* (2003); Office of the Attorney General for Western Australia, *Privacy Legislation for Western Australia Policy Research Paper* (2003) and J McGinty (Western Australian Attorney General), 'Public Consulted on Privacy Laws' (Press Release, 20 May 2003).

South Australia

Cabinet Administrative Instruction

2.53 There is no legislation that specifically addresses privacy in South Australia. 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.[84]

2.54 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 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.[85] 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.[86] 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.[87]

2.55 The ALRC has been informed that State Records of South Australia, in supporting the Privacy Committee of South Australia, is developing a guideline for matching and sharing personal information, and 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.[88]

Code of Fair Information Practice

2.56 South Australia also has a *Code of Fair Information Practice* based on the NPPs in the *Privacy Act*.[89] The Code applies to the South Australian Department of Health

---

84 South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

85 Ibid, Schedule. The Committee has reported that in 2004–05 it did not receive any complaints, although four pre-existing written complaints from members of the public underwent further deliberation: Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2004–05* (2005), [3.5].

86 Privacy Committee of South Australia, *Privacy Committee Members' Handbook Version 1.1* (2005), 16.

87 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 considered three exemptions in 2004–05: Privacy Committee of South Australia, *Annual Report of the Privacy Committee of South Australia 2004–05* (2005), [3.3].

88 State Records of South Australia, *Correspondence*, 9 August 2006.

89 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

and the Department of Human Services.[90] The Privacy Committee of South Australia has granted exemptions from the Cabinet Administrative Instruction to enable the Department of Health and the Department of Human Services to adopt the principles under the Code.[91]

Tasmania

Personal Information and Protection Act 2004 (Tas)

2.57 The *Personal Information and 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.[92] 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.[93]

2.58 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.

2.59 The Tasmanian regime is similar to legislation in other jurisdictions in that it prescribes exemptions for publicly available information and law enforcement information.[94] The obligations in relation to 'employee information', however, are different to the federal and other state and territory regimes—they allow job applicants and employees to benefit from the privacy obligations imposed on employers.[95] 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.[96]

---

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.

90 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].

91 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].

92 See definition of 'personal information custodian': *Personal Information Protection Act 2004* (Tas) s 3.

93 Ibid s 3.

94 Ibid ss 8, 9.

95 Ibid s 10.

96 Ibid s 13.

2.60 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.[97] 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.[98]

Charter of Health Rights

2.61 The *Health Complaints Act 1995* (Tas) requires the Tasmanian Health Complaints Commissioner to develop a *Charter of Health Rights*.[99] A Charter was developed and tabled in Parliament in 1999. The Charter applies to a wide range of health service providers. The Charter provides for six rights, including the right to confidentiality, privacy and security.[100] 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.[101]

2.62 The Tasmanian Health Complaints Commissioner administers the Charter.[102] The Tasmanian Health Complaints Commissioner has a number of functions including the receipt, assessment and resolution of complaints.[103] Complaints may be resolved by conciliation and through the use of enforceable agreements between a complainant and health service provider.[104] In 2004–05, the Commissioner reported that she resolved 44 privacy-related complaints out of a total of 693 complaints resolved in that period.[105] The ALRC has been advised that the Charter will be reviewed in late 2006.[106]

---

97 Ibid s 20.
98 Ibid s 22.
99 *Health Complaints Act 1995* (Tas) s 17.
100 Tasmanian Government Office of the Health Complaints Commissioner, *Tasmanian Charter of Health Rights and Responsibilities* (2006), 7.
101 Ibid, 7.
102 In Tasmania the same person holds the office of the Ombudsman and the Tasmanian Health Complaints Commissioner.
103 *Health Complaints Act 1995* (Tas) s 6(d) and pt 4.
104 Ibid pt 5.
105 Tasmanian Government Health Complaints Commissioner, *Ninth Annual Report 2004–05* (2005), 53. However, the category 'Privacy' includes assault, breach of confidentiality, discrimination, failure to ensure privacy, inconsiderate service and unprofessional conduct.
106 Tasmanian Government Health Complaints Commission, *Correspondence*, 10 August 2006.

Australian Capital Territory

2.63 The ACT public sector complies with an amended version of the *Privacy Act*.[107] The Office of the Privacy Commissioner (OPC) administers the Act on behalf of the ACT government.

Health Records (Privacy and Access) Act 1997 (ACT)

2.64 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.[108]

2.65 The Act gives people access to their own health records or any other record to the extent that it contains personal health information.[109] The Act imposes obligations on both the person requesting access to a health record[110] and the person who responds to a request for access.[111] 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.[112]

2.66 The ACT Community and Health Services Complaints Commissioner administers the Act.[113] Under Part 4, a complaint may be made to the Commissioner about an act or omission that is alleged to contravene the privacy principles. Complaints are administered under the *Community and Health Services Complaints Act 1993* (ACT).[114] In 2004, the Commissioner dealt with 29 complaints relating to access to, and disclosure of, personal health information.[115]

Human Rights Act 2004 (ACT)

2.67 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

---

107 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.
108 *Health Records (Privacy and Access) Act 1997* (ACT) s 5 and sch 1.
109 Ibid s 10.
110 Ibid s 12.
111 Ibid s 13.
112 Ibid s 14.
113 Ibid s 18.
114 Ibid s 21.
115 ACT Government Community and Health Services Complaints Commissioner, *Annual Report 2004–05* (2005), 28.

the Act, when a court is interpreting an ACT law it must adopt an interpretation 'consistent with human rights' as far as possible.[116]

Northern Territory

Information Act 2002 (NT)

2.68 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*.[117] 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,[118] or to court or tribunal proceedings.[119]

2.69 The Act also provides for approved codes of practice.[120] 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.[121]

2.70 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.[122] 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.[123]

2.71 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.[124] The Information Commissioner has the power to conduct a hearing in relation to the complaint and make a number of orders.[125] In 2004–05 the Information Commissioner received 13 complaints, six of which related to privacy issues.[126]

---

116 *Human Rights Act 2004* (ACT) s 30(1).
117 Northern Territory, *Parliamentary Debates*, Legislative Assembly, 14 August 2002 (P Toyne—Minister for Justice and Attorney-General).
118 *Information Act 2002* (NT) s 68.
119 Ibid s 69. For other exemptions see *Information Act 2002* (NT) pt 5 div 2.
120 *Information Act 2002* (NT) ss 72–80.
121 Ibid s 72.
122 Ibid s 81.
123 Ibid s 82.
124 Ibid s 104.
125 Ibid s 115.
126 Northern Territory Government Office of the Information Commissioner, *Annual Report 2004–05* (2005), 11.

Information Privacy Code of Conduct

2.72 The Northern Territory does not have health specific privacy legislation. However, in 1997 the Territory Health Services issued the *Territory Health Services Information Privacy Code of Conduct*.[127] The Code of Conduct includes 11 principles that are based on the IPPs in the *Privacy Act*.[128] 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).[129] However, legislative provisions take precedence over the *Code of Conduct*.[130]

Code of Health Rights and Responsibilities

2.73 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.[131] 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.

2.74 Principle 4 of the Code relates to personal information. It provides that people have a right to information about their health, care and treatment. However, they do not have 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.

2.75 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,[132] and may receive complaints from the Information Commissioner.[133] The Health and Community Services Complaints Review Committee may review decisions by the Commissioner.[134] In 2004–05, the Commission reported that it

---

127 Northern Territory Government Department of Health, *Information Privacy Code of Conduct* (1997).
128 Ibid, [1.6].
129 Ibid, [1.3].
130 Ibid, [1.3.2], [1.5].
131 Northern Territory Government Health and Community Services Complaints Commission, *Code of Health Rights and Responsibilities*, 6.
132 *Health and Community Services Complaints Act 1998* (NT) pt 6.
133 Ibid s 25A.
134 Ibid pt 9.

received eight complaints relating to access to records and seven complaints relating to 'privacy/confidentiality'.[135]

Proposed health privacy legislation

2.76 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*.[136] 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 was to 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.[137]

Other relevant state and territory legislation

2.77 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.

2.78 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.[138] 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.

2.79 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

---

135 Northern Territory Government Health and Community Services Complaints Commission, *Seventh Annual Report 2004–2005* (2005), 77.

136 Northern Territory Government Department of Health and Community Services, *Protecting the Privacy of Health Information in the Northern Territory*, Discussion Paper (2002).

137 Ibid, Ch 8.

138 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.

under the Act or will only be released after a consultation process.[139] Freedom of information legislation also ensures that records held by the Government concerning the personal affairs of members of the public are not incomplete, incorrect, out-of-date or misleading.[140]

2.80 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.[141]

2.81 Some privacy protection is also provided in state and territory legislation regulating the use of listening and other surveillance devices,[142] and telecommunications interception.[143]

Privacy rules, codes and guidelines

Legislative rules, codes and guidelines

2.82 Legislation other than the *Privacy Act* requires the development of privacy codes or guidelines.[144] 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 which customers have in relation to using or blocking the display of CND information from their services; charges which may apply in relation to enabling or blocking the display of CND information to CND services; and measures to be

---

139 *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 and 33.

140 *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.

141 *Public Records Act 1973* (Vic) s 9; *Public Records Act 2002* (Qld) ss 16 and 18; *State Records Act 2000* (WA) s 49; *Archives Act 1983* (Tas) s 15; *Territory Records Act 2002* (ACT) s 28.

142 *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).

143 *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).

144 For other examples of legislative codes and guidelines see Ch 7.

undertaken by suppliers to ensure that the public is aware of CND services and their implications.[145]

2.83 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.[146]

Non-legislative rules, codes and guidelines

2.84 In addition to legislative protection of personal information, organisations will often develop and publish privacy guidelines that are not required by legislation.[147] For example, the private sector provisions of the *Privacy Act* exempts 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.[148] The Australian Press Council (APC) has developed a set of eight privacy standards to regulate the handling of personal information.[149] 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.

2.85 The ALRC is interested in receiving information on other examples of non-legislative privacy codes, guidelines or standards.

National consistency

2.86 Australia is yet to achieve uniformity in the regulation of personal information. A key concern of recent inquiries has been that Australian privacy laws are multi-

145 Australian Communications Industry Forum, *Industry Code—Calling Number Display*, ACIF C522 (2003).

146 Reproduced in Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), Attachment A.

147 For other examples of non-legislative codes and guidelines see Ch 7.

148 *Privacy Act 1988* (Cth) s 7B(4).

149 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 16 June 2006. The Standards adopt the *Privacy Act* definition of 'personal information'.

layered, fragmented and inconsistent.[150] For example, the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (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.[151]

2.87 Chapter 7 documents various problems caused by inconsistency and fragmentation in privacy regulation. Many of these problems relate to the difficulty in identifying the sources of privacy obligations, or the time and money spent identifying sources of privacy obligations and complying with disparate laws and inconsistent privacy standards in different jurisdictions. There is also the issue of the effectiveness of the protection of privacy in the absence of a national regime.

2.88 A threshold issue is whether national consistency should be one of the goals of the regulation of personal information. Both the Senate Committee privacy inquiry and the OPC Review 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.[152] The OPC Review also made a number of recommendations directed to national consistency.[153]

2.89 The ALRC is interested in hearing whether national consistency is a desirable goal, or when circumstances may exist where inconsistency is justified. For example, particular industry sectors may require different laws to regulate the handling of personal information on the basis that greater national consistency is considered desirable. The following section considers various methods to achieve national consistency in the regulation of personal information.

---

150 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 and 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 and 4.48. Chapter 7 discusses inconsistency and fragmentation in the regulation of personal information.

151 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.6].

152 Ibid, Rec 3.

153 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.

Models for dealing with inconsistency and fragmentation

2.90 This section of the chapter considers models for dealing with inconsistency and fragmentation in the regulation of personal information. These methods include national legislation, a cooperative scheme, mechanisms for dealing with multiple regulators, privacy impact statements, and the establishment of a permanent standing body to consider privacy issues. The ALRC welcomes views on whether these options are appropriate and on whether there are other methods that may assist national consistency.

National legislation

2.91 The Australian Parliament could pass national legislation regulating the handling of personal information throughout Australia. The power to enact this legislation would be based on a range of constitutional powers, including the external affairs power.[154] 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.

2.92 This option raises a range of issues. For example, consideration would need to be given as to how this legislation would interact with other federal legislation that regulates the handling of personal information by the Australian Government public sector, such as the FOI Act and the *Archives Act*. As discussed in Chapter 7, one option would be to incorporate the provisions of the *Privacy Act*, FOI Act and the *Archives Act* into one Act. A further issue is the scope of the Act. Provisions dealing with the handling of personal information under other federal legislation, such as the *Telecommunications Act*, could be incorporated into the Act. Another issue is whether the national legislation would deal with health information.[155]

2.93 If national legislation extended to the state and territory public sectors consideration would also need to be given as to how this legislation would interact with state and territory legislation such as freedom of information and public records legislation.

2.94 As discussed above, state and territory public sector authorities are excluded from the operation of the *Privacy Act*. However, s 6F of the *Privacy Act* provides that a state and territory may request that their public sector authorities be brought under the Act by regulation. This mechanism could be used to extend national privacy legislation to the state and territory public sectors if it were considered appropriate to do so. Another option for consideration is for national legislation to 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

154 See discussion above.
155 Other options to achieve national consistency in the handling of health information are discussed in Ch 8.

conform to the specified federal minimum standards. There are examples of roll-back provisions in various areas of the law.[156]

A cooperative scheme

2.95 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.[157] Commonwealth-state cooperative schemes may be categorised into three types: reference to the Commonwealth, mirror legislation and complementary law regimes.[158]

2.96 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, while a cooperative scheme could address the handling of personal information in each of the state public sectors. Another option would be to have a state cooperative scheme that only related to the private sector. Further issues include: what types of information would be regulated by a cooperative scheme, and how such a scheme would interact with other federal and state laws relevant to the handling of personal information.

Reference to the Commonwealth

2.97 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.

2.98 The states have referred a number of matters to the Commonwealth including corporations and counter-terrorism.[159] 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

---

156 *Gene Technology Act 2000* (Cth) s 14; *Environmental Protection (Sea Dumping) Act 1981* (Cth) s 9.

157 J Ledda, 'The Drafter's Guide to Cooperative Schemes' (Paper presented at Drafting Forum 2001, Melbourne) in M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 3.

158 Ibid, 3.

159 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). 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.

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).[160] 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 quite 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

2.99 Mirror legislation usually refers to a system where one jurisdiction enacts a law that is then enacted in similar terms by other jurisdictions.[161] 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.*

2.100 Each Australian state could pass similar legislation to regulate the handling of personal information by the private sector, or that state's public sector. However, mirror legislation can result in inconsistency both at the time the legislation is enacted and as laws are amended.[162] One option for dealing with this is to have a central body to maintain uniformity. In *Uniform Evidence Law* (ALRC 102) the ALRC recommended in relation to the uniform Evidence Acts that:

> the Standing Committee of Attorneys-General (SCAG) should adopt an Intergovernmental Agreement which provides that, subject to limited exceptions, any proposed changes to the uniform Evidence Acts must be approved by SCAG. 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.[163]

Complementary law regime

2.101 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.[164] An example of a complementary applied law scheme is the agricultural and veterinary chemicals legislation. The Australian Parliament enacted the *Agvet 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. The *Competition Code* is another

---

160 Explanatory Memorandum, Terrorism (Commonwealth Powers) Bill 2003 (Vic).

161 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 4–5.

162 See, eg, Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Ch 1.

163 Ibid, Rec 2–1.

164 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 8.

example of a complementary applied law regime.[165] 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.[166]

> 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.[167]

2.102 For example, the Australian Parliament could enact legislation dealing with the handling of personal information by the Australian Government public sector which could then be adopted by the states to apply to state public sectors. However, uniformity can be reduced 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.[168]

2.103 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.[169] 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.

2.104 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.[170]

Other methods to achieve national consistency

Binding codes

2.105 The OPC Review suggested that one way of overcoming the problems caused by inconsistent state and territory legislation regulating a particular activity is to

---

165 See *Competition Code* (Cth) pt XIA.

166 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005), 9.

167 Ibid, 10.

168 Ibid, 10.

169 See, eg, *Classification (Publications, Films and Computer Games) Enforcement Act 1995* (Vic).

170 See, eg, *Gene Technology Act 2000* (Cth); *Gene Technology (New South Wales) Act 2003* (NSW) (an applied law); *Gene Technology Act 2001* (Vic) (mirror legislation).

provide for a power within the *Privacy Act* to develop binding codes.[171] The OPC Review considered that binding codes could be used to regulate a number of areas, at a national level, including residential tenancy database operators.[172]

2.106 The OPC Review considered three models for binding codes.[173] The first model involves the Attorney-General, after identifying the need for a code in a specific sector, asking the Privacy Commissioner to commence a process to develop a code in consultation with key stakeholders. The second model is that set out in the *Trade Practices Act*, which provides for the Minister to declare by regulation that a code is mandatory for a particular industry.[174] The third model is that the Privacy Commissioner, at his or her own initiative, could make a binding code in appropriate circumstances and after stakeholder consultation. A similar model is contained in the *Telecommunications Act*.[175] One issue is whether the power to make binding codes would further contribute to the complexity, inconsistency and fragmentation of privacy regulation. Binding codes are further considered in Chapter 6.

Non-binding guidelines

2.107 Another option for consideration is the making of non-binding guidelines. The Privacy Commissioner publishes a number of non-binding guidelines.[176] 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,[177] 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*.[178]

Rules, codes and guidelines

2.108 The potential for inconsistencies and complexities to arise because of the development of privacy rules, privacy codes and guidelines is discussed in Chapter 7. One option for consideration is whether the Australian Government should amend the *Privacy Act* to provide that all privacy rules, privacy codes and guidelines are required to be approved by the Privacy Commissioner.

---

171 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 6.

172 Ibid, 159.

173 Ibid, 46–47.

174 *Trade Practices Act 1974* (Cth) s 51AE.

175 *Telecommunications Act 1997* (Cth) s 125.

176 See, eg, Office of the Federal Privacy Commissioner, *Guidelines for the Use of Data-Matching in Commonwealth Administration* (1998) <www.privacy.gov.au> at 2 September 2006, discussed above.

177 Office of the Federal Privacy Commissioner, *Guidelines on Workplace E-mail, Web Browsing and Privacy* (2000) <www.privacy.gov.au> at 20 April 2006.

178 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.

Guidance on the interaction of legislation

2.109 The complex interaction between the *Privacy Act* and other federal, state and territory regimes that regulate personal information has been detailed in this chapter and other chapters.[179] 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.[180] 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*.

2.110 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.[181] This recommendation has not been implemented to date. The Attorney-General's Department has issued guidance on how the FOI Act interacts with the *Privacy Act*.[182]

Privacy impact statements and assessments

2.111 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,[183] 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.[184]

2.112 One issue is whether a 'privacy impact statement' should accompany any federal, state and territory government proposal to introduce legislation that impinges on privacy.[185] Such a statement could include a Privacy Impact Assessment and an

---

179 See, eg, Chs 7, 10.

180 The Privacy Commissioner has power to issue such guidance under *Privacy Act 1988* (Cth) s 27(1)(e).

181 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).

182 Australian Government Attorney-General's Department, *Freedom of Information Memorandum 93: FOI and the Privacy Act* (1992).

183 Australian Government Office of Regulation Review, *A Guide to Regulation—Second Edition: December 1998* (1999), B3–B4.

184 Ibid, B2–B3.

185 Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

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. See Chapter 6 for further discussion of Privacy Impact Assessments for new legislation.

Scrutiny of legislation

2.113 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*.[186] While this function may be used to ensure that federal legislation remains consistent, it may not assist national consistency. The establishment of a permanent standing body to consider national consistency in privacy regulation is considered below.

Clarify jurisdiction to investigate complaints

2.114 As noted in Chapter 7, a number of issues may arise because more than one body is responsible for the regulation of personal information. There are multiple privacy regulators in particular industry sectors as well as across jurisdictions. 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.

MOUs and transferral of complaints

2.115 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 enforcement.[187] One method of achieving this is the development of memorandums of understanding between privacy regulators in relation to enforcement of privacy laws. Another option for consideration is the provision of powers to transfer complaints between industry specific regulators, state and territory regulators and the Privacy Commissioner.[188]

---

186 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.

187 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.

188 See, eg, *Privacy Act 1988* (Cth) s 50; *Telecommunications Act 1997* (Cth) s 515A; *Ombudsman Act 1974* (NSW) s 6(4A).

Permanent standing body

2.116 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.[189] 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.[190] 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.[191]

2.117 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 national health privacy code. 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.[192]

2.118 The proposal for a permanent standing body to ensure national consistency in the regulation of personal information 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.

2.119 One option for consideration is to broaden the membership and functions of the Privacy Advisory Committee established under the *Privacy Act*.[193] Another option would be to formalise 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. To be an APPA member, authorities have to be accredited to the international meeting of Commissioners and come from Asia or the Western Pacific. 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.[194]

---

189 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 43.

190 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.

191 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.

192 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.

193 The Privacy Advisory Committee is discussed in Ch 6.

194 Asia Pacific Privacy Authorities Forum, *Statement of Objectives* (2005).

2.120 It may be more appropriate to establish a body that is independent of the Privacy Commissioner and that is directed to consider specifically the issue of national consistency. The functions of such a body could include: ensuring national consistency in the regulation of personal information; facilitating the sharing of knowledge and resources amongst privacy regulators; the development of cooperative arrangements for the enforcement of privacy laws; scrutiny of legislation that impacts on the privacy of individuals; and the promotion of best practice by privacy regulators.

Overseas federations

2.121 The United States, Germany and Canada are three examples of federations that regulate the handling of personal information. Unfortunately, none of these jurisdictions provide a model for nationally consistent privacy laws. Privacy regulation occurs at both a federal and state level in the United States. The primary legislation is the federal *Privacy Act of 1974* (US), which protects records held by United States government agencies.[195] Health privacy is regulated at both the federal and state level.[196] The states also have enacted legislation dealing with a range of other matters including financial privacy and identity theft.[197]

2.122 The *Federal Data Protection Act 1990* (Germany) covers the handling of personal data collected by public federal and state authorities (where there is no state regulation) and by the private sector if the organisation processes and uses data for commercial or professional purposes.[198] All 16 Länder have their own data protection regulations that cover the public sector of the Länder administrations.

2.123 In Canada, privacy is regulated at both the federal and provincial levels. At the federal level, privacy is protected by the *Privacy Act 1982* (Canada) and the *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act). The *Privacy Act 1982* (Canada) regulates the handling of personal information held by federal public agencies.[199] The PIPED Act regulates private sector organisations that process personal information 'in the course of a commercial activity' and for federally regulated employers with respect to their employees.[200] Public sector legislation covering government bodies exists in all provinces and territories.

2.124 Many Canadian provinces have specific laws to protect personal information, including health-specific privacy laws and consumer credit reporting laws. Section 26(2)(b) of the PIPED Act provides that the Governor-in-Council may, by order, exempt an organisation, activity or class of organisations or activities from the

---

195 *Privacy Act 1974* 5 USC § 552a (US).

196 See, eg, United States Government Department of Health and Human Services, *Standards for Privacy of Individually Identifiable Health Information; Final Rule* (2000) and the *Civil Code* (California) § 1798.91, relating to the regulation of health information for direct marketing purposes.

197 See, eg, *Financial Information Privacy Act* Financial Code (California) §§ 4050–4060.

198 *Federal Data Protection Act 1990* (Germany).

199 *Privacy Act* RS 1985, c P-21 (Canada).

200 *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada).

application of the Act if satisfied that legislation of a province that is 'substantially similar' to the PIPED Act applies to that organisation.

Question 2–1 Is national consistency in the regulation of personal information important? If so, what are the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia?

3. The *Privacy Act 1988* (Cth)

Contents

Introduction

3.1 The Privacy Bill 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.

3.2 The Preamble to the Bill makes clear that the legislation was intended to implement Australia's obligations relating to privacy under the United Nations

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 12.

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).

3.3 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.

3.4 The *Privacy Act 1988* (Cth), in its original form, set out the Information Privacy Principles (IPPs), which regulated the collection, handling and use 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 also provided guidelines for the collection, handling and use 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]

3.5 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 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]

3.6 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.[9]

---

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 12.

7 *Australian Capital Territory Government Service (Consequential Provisions) Act 1994* (Cth).

8 *Privacy Amendment Act 1990* (Cth).

9 Part IIIA of the *Privacy Act 1988* (Cth), which deals with credit reporting, is not addressed in detail in this Issues Paper. It will be addressed in a separate Issues Paper.

3.7 In 2000, the Act was amended to extend coverage to private sector organisations more generally.[10] This amendment introduced the National Privacy Principles (NPPs) into the legislation. The NPPs were developed following consultation with business, consumers and other stakeholders.[11] 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.[12]

3.8 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.

3.9 As discussed below, and in Chapters 4, 5 and 7 of this Issues 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 with certainty whether a particular agency or organisation is covered by the *Privacy Act* and, if so, to what extent. In addition, the drafting of some exemptions, such as exempt acts and practices set out in s 7, is complex and difficult to understand. A number of commentators have been critical of this complexity[13] and it seems undesirable in an Act intended to protect individuals' personal information. An individual is unlikely to be able to take action to protect his or her personal information if it is difficult to ascertain what acts and practices of which agencies and organisations are covered by the legislation.

Question 3–1 Is the structure of the *Privacy Act* logical? Does the *Privacy Act* need to be redrafted to achieve a greater degree of simplicity and clarity?

3.10 This chapter is intended to give an overview of the *Privacy Act* in its current form and to raise some basic issues in relation to the Act, for example, whether the name of the Act is accurate and appropriate. Other chapters of this Issues Paper will examine particular parts of the Act in more detail.

---

10 *Privacy Amendment (Private Sector) Act 2000* (Cth).

11 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).

12 *Privacy Amendment (Office of the Privacy Commissioner) Act 2000* (Cth).

13 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 8 August 2006, [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).

The name of the Act

3.11 The *Privacy Act* is 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.[14]

3.12 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 collection and use of personal information by the public sector. The New Zealand *Privacy Act 1993* regulates the collection and use of personal information in both the public and the private sector.

3.13 However, names given to similar legislation in a number of other jurisdictions 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);
- *Personal Information Protection and Electronic Documents Act 2000* (Canada).[15]

3.14 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

---

14 Commonwealth, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 51 (K Curtis—Privacy Commissioner).

15 The *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) regulates the collection and use of personal information by the private sector.

Parliament, and may act to publicise the legislation locally and internationally.[16] Names that do not accurately describe the scope of legislation may mislead the public into believing that a law covers particular areas that, in fact, it does not. 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*.

Question 3–2 Insofar as the *Privacy Act* is primarily concerned with data protection, is the name of the *Privacy Act* accurate and appropriate?

The objects of the Act

3.15 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.

3.16 Section 3 of the *Privacy Amendment (Private Sector) Act 2000* (Cth) 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.

3.17 The *Information Privacy Act 2000* (Vic)[17] and the *Information Act 2002* (NT)[18] expressly set out the objects of the legislation but the *Privacy and Personal Information Protection Act 1998* (NSW) and the *Personal Information Protection Act 2004* (Tas) do not.

16 M Whisner, 'What's in a Statute Name?' (2005) 97 *Law Library Journal* 169, 183.
17 *Information Privacy Act 2000* (Vic) s 1.
18 *Information Act 2002* (NT) s 3.

3.18 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 express 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).

3.19 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.[19]

3.20 In a paper presented to the 4th Australasian Drafting Conference, Paul Lanspeary of the Office of Parliamentary Counsel explained that:

> Courts look at objects clauses to see whether they can adopt a purposive approach to interpretation to particular legislation. In some cases, they may have a significant effect on how a question of statutory interpretation is resolved, or at least may be quite useful to a court in arriving at a sensible outcome … However a court will not use an objects clause to override what it considers to be the clear and unambiguous text of an operative provision.[20]

3.21 Section 15AA of the *Acts Interpretation Act* 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.

Question 3–3 Is there some benefit in amending the *Privacy Act* to include the objects of the legislation? If so, what should be included in the objects clause?

Some important definitions

3.22 Part II of the *Privacy Act* sets out a number of important definitions. While these will be discussed in detail, where relevant, throughout this Issues Paper, some core definitions are described in general terms below.

---

19 Office of Parliamentary Counsel, *Working with the Office of Parliamentary Counsel: A Guide for Clients* (2nd ed, 2002), [116]–[117].

20 P Lanspeary, 'Statutory Interpretation for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005).

Personal information

3.23 Central to the regime established by the *Privacy Act* is the definition of 'personal information'. This is because the IPPs and NPPs only apply to personal information. 'Personal information' 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'.[21]

3.24 Personal information includes written or electronic records about individuals such as social security records and doctors' records, but 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.

3.25 The OECD Guidelines[22] and the Council of Europe Convention[23] define 'personal data' as 'any information relating to an identified or identifiable individual'. 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* (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.[24]

3.26 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.[25] 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

---

21 *Privacy Act 1988* (Cth) s 6(1).

22 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), art 1.

23 *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.

24 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.

25 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.

individuals—and to develop profiles of those individuals—that is not linked to their legal identity such as their name and address. The Committee noted that it may be more useful to work with concepts such as biographical data, identifiers linked to individuals or to terminals and points of contact.[26]

3.27 The Revised Explanatory Memorandum for the Privacy Amendment (Private Sector) Bill 2000 emphasised the need for the privacy framework to be flexible and technology neutral so that it could adjust to changing circumstances and emerging technologies.[27] The Senate Committee also expressed the view that it was desirable for the *Privacy Act* to remain as technologically neutral as possible and that it was viable to update the Act in a technologically neutral manner to accommodate new and emerging technologies.[28]

3.28 Another issue that arose in the context of the Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act* (OPC Review) was the difficulty of ascertaining whether personal information was 'identified', 'identifiable' or 'de-identified'. The *Privacy Act* only protects personal information if the information is about a person 'whose identity is apparent, or can reasonably be ascertained, from the information or opinion'. The Australian Consumers Association expressed the view that the whole issue of de-identified data needs to be re-examined and that the OPC should provide guidelines that set out a clear working definition of 'de-identified' data.[29]

3.29 Chapter 8 considers this issue in the context of health information and health and medical research. In particular, the chapter discusses to what extent health information that has been de-identified but may be re-identifiable should be protected by the *Privacy Act.* The ALRC would be interested in views on whether the current formulation of the concept of 'identifiable' personal information in the *Privacy Act* is appropriate and effective.

3.30 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.[30]

---

26 Y Poullet, *Report on the Application of Data Protection Principles to the Worldwide Telecommunications Networks* (2004) Council of Europe, 33.

27 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 10.

28 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.11].

29 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.

30 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.

Sensitive information

3.31 'Sensitive information' is a sub-set of personal information and is given a higher level of protection under the NPPs. 'Sensitive information' is defined as health information about an individual or personal 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;
- criminal record.[31]

3.32 The same classes of information are included in the definitions of sensitive information in the Victorian, Tasmanian and Northern Territory privacy legislation although 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).[32] The *Privacy and Personal Information Protection Act 1998* (NSW) does not include a definition of sensitive information.

3.33 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'.[33] The EU Directive does refer to 'sensitive data' but does not define the term.[34]

3.34 In *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC)

---

31 *Privacy Act 1988* (Cth) s 6(1). The definition of 'health information' is discussed in Ch 8.

32 *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.

33 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19].

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), arts 34, 70.

considered the definition of sensitive information. They came to the conclusion that the existing 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. The ALRC and AHEC recommended that:

> The Commonwealth should amend s 6 of the *Privacy Act* to define 'sensitive information' to include human genetic test information.[35]

3.35 The Australian Government expressed support for this recommendation and an amendment to the *Privacy Act* came into force in September 2006.[36]

3.36 Stakeholders have also suggested that the definition is not adequate in other ways as it excludes information that is made sensitive by the context in which the information is found, for example, the street address of an individual in a witness protection program, and does not include sensitive information such as financial information about individuals.[37]

Records and generally available publications

3.37 The IPPs and NPPs protect personal information that is held, or collected for inclusion, in a 'record'. A record is defined as a document, a database, or a photograph or other pictorial representation.[38] The definition of record excludes a range of things such as items kept in libraries, art galleries or museums for reference, study or exhibition and generally available publications—that is, books, magazines or other publications that are generally available to 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 IPPs and NPPs.[39]

Agencies and organisations

3.38 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.[40] There are a number of exemptions to this definition discussed below and in Chapter 5.

3.39 The NPPs regulate the activities of private sector organisations. 'Organisation' is defined as an individual, a body corporate, a partnership, any other unincorporated

---

35 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.
36 *Privacy Legislation Amendment Act 2006* (Cth).
37 Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005.
38 *Privacy Act 1988* (Cth) s 6(1).
39 Ibid ss 14, 16B.
40 Ibid s 6(1).

association or a trust.[41] There are a number of exemptions to this definition discussed below and in Chapter 5.

Acts and practices

3.40 Finally, 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 Chapter 5.

Question 3–4 Are the definitions in the *Privacy Act* adequate and appropriate? For example, are the definitions of 'personal information' and 'sensitive information' in the *Privacy Act* adequate and appropriate?

Deceased individuals

3.41 The *Privacy Act* does not protect the personal information of deceased individuals. The term *individual* is defined as 'a natural person'.[42] 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.[43]

3.42 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.[44]

41 Ibid s 6C.
42 Ibid s 6(1).
43 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 281.
44 P Roth, 'Privacy Proceedings and the Dead' (2004) 11 *Privacy Law & Policy Reporter* 50.

3.43 By way of contrast, the *Freedom of Information Act 1982* (Cth) protects the personal information of deceased persons from unreasonable disclosure.[45] In New South Wales the privacy and health privacy legislation covers personal information about individuals who have been dead for not more than 30 years[46]—this is consistent with the 30 year period after which government archival records are generally open to public access.[47] Victorian health privacy legislation also covers personal information of individuals who have been dead for not more than 30 years.[48] Tasmanian privacy legislation extends to the personal information of a person who has been dead for not more than 25 years[49] and ACT health privacy legislation provides that privacy principles apply to deceased individuals without imposing any time restrictions.[50]

3.44 In ALRC 96, the ALRC and AHEC 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.[51]

3.45 This was on the basis that information privacy protection should extend to genetic information about deceased individuals because of the implications that the collection, use or disclosure of this information may have for living genetic relatives.[52] 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*.[53] 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.[54]

3.46 The OPC review noted that extending the Act to cover the personal information of those who have died would require some reworking of provisions and principles relating to consent and the lodging of complaints. It recommended that:

---

45 *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).

46 *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(a); *Health Records and Information Privacy Act 2002* (NSW) s 5(3)(a).

47 *Archives Act 1983* (Cth) s 3(7).

48 *Health Records Act 2001* (Vic) ss 3(1), 95.

49 *Personal Information Protection Act 2004* (Tas) s 3.

50 *Health Records (Privacy and Access) Act 1997* (ACT) ss 4, 27 and dictionary (definition of 'consumer').

51 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.

52 Ibid, [7.90].

53 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 2 August 2006.

54 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 4.

> If the National Health Privacy Code is adopted into the Privacy Act (see recommendation 13), then protection for health information under these provisions would extend to deceased persons. Also, the Australian Government's response to the Australian Law Reform Commission and the Australian Health Ethics Committee's Inquiry into the protection of human genetic information in Australia may have implications for the Privacy Act. In addition, the Australian Government should consider as part of a wider review (recommendation 1) whether the jurisdiction of the Privacy Act should be extended to cover the personal information of deceased persons.[55]

3.47 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. In it's submission to the OPC review, the Australian Privacy Foundation expressed the view that any personal information about deceased individuals has the potential to cause distress to relatives and that consideration should be given to extending the protection of the *Privacy Act* to cover all the personal information of deceased individuals.[56]

Question 3–5 Should the definition of 'personal information' in the *Privacy Act* be amended to include personal information of the deceased?

Exemptions and exceptions

3.48 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 Issues Paper refers to *exceptions* where they arise under the IPPs and NPPs and *exemptions* in other circumstances. A number of these have been the subject of criticism and are discussed in detail in Chapters 4 and 5.

3.49 The acts and practices of some Australian Government agencies—including the intelligence agencies: the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO) and the Office of National Assessments (ONA)—are completely exempt from the *Privacy Act*.[57]

3.50 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*,

---

55 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.

56 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

57 *Privacy Act 1988* (Cth) s 7.

only some acts and practices of federal courts are covered by the Act.[58] Acts and practices in relation to administrative functions such as personnel files, operational and financial records, and mailing lists, for example, are covered.[59] However, acts done and practices engaged in as part of the courts' judicial functions are not covered.

3.51 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.[60] Some small businesses that pose a higher risk to privacy—for example, small businesses that hold health information and provide health services or those that trade in personal information—are covered by the Act.[61] Other small business operators may choose to opt in to the regime[62] or may be brought into the regime by regulation.[63]

3.52 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.[64]

3.53 The Act does not apply to personal information being collected, used or disclosed for personal, family or household purposes.[65]

3.54 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.[66] 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.[67] 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.

3.55 Media organisations are exempt in relation to acts or practices in the course of journalism.[68] A media organisation is an organisation whose activities consist of or

---

58 Ibid s 7.
59 *I v Commonwealth Agency* [2005] PrivCmrA 6.
60 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
61 *Privacy Act 1988* (Cth) s 6D(4).
62 Ibid s 6EA.
63 Ibid s 6E.
64 Ibid s 6F.
65 Ibid ss 7B(1), 16E.
66 Ibid s 7B(3).
67 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
68 *Privacy Act 1988* (Cth) s 7B(4).

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.[69]

3.56 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 representatives may also be exempt where their acts or practices are related to the political process.[70]

3.57 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 defined 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.

3.58 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

3.59 The Act contains a set of 11 Information Privacy Principles (IPPs) based on the OECD Guidelines.[71] The IPPs are a central feature of the *Privacy Act* and are discussed in detail in Chapter 4. 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.[72] 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 it is compulsory to provide the information and the agency's usual practices in relation to disclosure of such

69 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
70 *Privacy Act 1988* (Cth) s 7C.
71 Ibid s 14.
72 Ibid s 14, IPP 1.

information.[73] The IPPs require agencies to ensure that information is relevant, up-to-date and complete.[74]

3.60 Agencies must also store information securely[75] and provide information about the type of personal information they hold.[76] Subject to certain exceptions, agencies must provide individuals with access to personal information about them and correct information to ensure that it is accurate, up-to-date, relevant, complete and not misleading.[77] Agencies must generally seek an individual's permission to use or disclose information for a purpose that is not directly related to the reason it was collected.[78] As noted above, the IPPs contain a range of exceptions.

National Privacy Principles

3.61 The Act contains a set of 10 National Privacy Principles (NPPs)—developed in consultation with private sector organisations—that apply in the private sector where no approved privacy code has been put in place.[79] The NPPs are discussed in detail in Chapter 4. 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.[80] Sensitive information may generally only be collected with consent.[81]

3.62 Organisations only may 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.[82] Organisations must take reasonable steps to ensure that information is accurate, complete and up-to-date[83] and must protect the information from misuse and loss and from unauthorised access, modification or disclosure.[84] Organisations must also take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed.[85]

---

73 Ibid s 14, IPP 2.
74 Ibid s 14, IPP 3.
75 Ibid s 14, IPP 4.
76 Ibid s 14, IPP 5.
77 Ibid s 14, IPP 7.
78 Ibid s 14, IPPs 10, 11.
79 Ibid sch 3.
80 Ibid sch 3, NPP 1.
81 Ibid sch 3, NPP 10.
82 Ibid sch 3, NPP 2.
83 Ibid sch 3, NPP 3.
84 Ibid sch 3, NPP 4.
85 Ibid sch 3, NPP 4.

3.63 On request, organisations are required to let individuals know what sort of personal information they hold and how they handle that information,[86] and to give individuals access to the information held about them unless particular exceptions apply.[87] There are limits on the use of government identifiers by the private sector[88] and on transferring personal information overseas.[89] 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.[90] As noted above, the NPPs contain a range of exceptions.

Approved privacy codes

3.64 The *Privacy Amendment (Private Sector) Act* 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 approves a privacy code, it replaces the NPPs for those organisations bound by the code.[91] Codes may also set out procedures for making and dealing with complaints. Such codes must appoint an independent adjudicator to whom complaints may be made.[92]

3.65 The aim of the amending Act was to encourage private sector organisations and industries to develop privacy codes of practice[93] but 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 now been revoked. Privacy codes are discussed further in Chapter 6.

Interference with privacy

3.66 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.[94] An act or practice by an organisation that breaches an NPP or, where one is in place, an approved privacy code is an interference with privacy.[95] An

86 Ibid sch 3, NPP 5.
87 Ibid sch 3, NPP 6.
88 Ibid sch 3, NPP 7.
89 Ibid sch 3, NPP 9.
90 Ibid sch 3, NPP 5.
91 Ibid s 16A.
92 Ibid s 18BB.
93 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).
94 *Privacy Act 1988* (Cth) s 13.
95 Ibid s 13A.

interference with privacy may also arise in other areas including: the handling of Tax File Number (TFN) information, data-matching, and credit reporting.

Credit reporting

3.67 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 credit reporting[96]—to provide safeguards for individuals in relation to consumer credit reporting.[97] 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 information privacy principles to the handling of personal credit information.[98] The current Code includes amendments made following a number of reviews and is dated March 1996.[99]

3.68 The credit reporting provisions have been the subject of criticism[100] and will be considered in detail in a separate Issues Paper.

Tax file numbers

3.69 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.[101] 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 complaint to the Privacy Commissioner.[102] 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.[103]

---

96 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) <www.privacy.gov.au> at 21 April 2006.

97 *Privacy Amendment Act 1990* (Cth).

98 *Privacy Act 1988* (Cth) s 28A.

99 Office of the Federal Privacy Commissioner, *Credit Reporting Code of Conduct* (1991) <www.privacy.gov.au> at 21 April 2006.

100 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].

101 TFNs are discussed in detail in Ch 12.

102 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.

103 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).

The Privacy Commissioner

3.70 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.[104] The powers and role of the Privacy Commissioner are examined in detail in Chapter 6.

The Office of the Privacy Commissioner

3.71 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*.[105] The Office consists of a number of sections as follows:

- the Hotline;
- the Compliance Section;
- the Policy Section; and
- Corporate and Public Affairs.

3.72 The Hotline Section provides assistance to individuals in relation to their rights under the *Privacy Act* and related legislation. The section also provides advice to federal and ACT government agencies and private sector organisations on how to comply with the Act and related legislation.

3.73 The Compliance Section investigates complaints from individuals against federal and ACT government agencies and private sector organisations. Compliance 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 federal and ACT government agencies, credit providers and credit reporting agencies. Compliance also conducts audits under s 309 of the *Telecommunications Act 1997* (Cth).

3.74 The Policy Section provides guidance and advice to federal and ACT government agencies and private sector organisations on privacy issues; examines and makes submissions on proposed legislation and comments on inquiries that have significant privacy implications; and also seeks to inform itself of technological and social developments that affect individual privacy. The Corporate and Public Affairs section assists the Office in communicating with stakeholders through publications, media relations, secretariat support, speech writing, events and the Office website.[106]

---

104 *Privacy Act 1988* (Cth) ss 19–25.
105 Ibid ss 19, 26A.
106 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 3 August 2006.

The functions of the Privacy Commissioner

3.75 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;
- publishing various guidelines, including binding guidelines, on the development of privacy codes and the use of health information for medical research;[107] and
- providing advice to the Minister and others.[108]

3.76 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 relation to 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;[109]
- *National Health Act 1953* (Cth) in relation to regulating the handling of Medicare and Pharmaceutical Benefits Program claims information. The Privacy

107 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 8.
108 *Privacy Act 1988* (Cth) s 28A.
109 These guidelines are discussed further in Chs 6 and 7.

Commissioner is required to issue guidelines under the Act and has the power to investigate acts or practices that may breach the guidelines;[110]

- *Crimes Act 1914* (Cth) in relation to 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;[111] and

- *Telecommunications Act 1997* (Cth) in relation to 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.[112]

3.77 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 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.[113]

Investigations

3.78 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.[114] In conducting such investigations, the Commissioner has power to require the production of documents and information, and may also require people to appear and answer questions.[115] The Commissioner may examine such witnesses on oath or affirmation.[116]

3.79 The Privacy Commissioner may make various determinations where there has been a breach of the IPPs or NPPs.[117] 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 are not, however, binding between the

---

110 These guidelines are discussed further in Chs 6 and 8.
111 These functions are discussed further in Ch 6.
112 Office of the Privacy Commissioner, *About the Office* <www.privacy.gov.au/about/> at 3 August 2006. These functions are discussed further in Chs 6 and 10. The question of whether these functions should be consolidated into the *Privacy Act* is considered in Ch 6.
113 *Privacy Act 1988* (Cth) s 29.
114 Ibid pt V.
115 Ibid s 44.
116 Ibid s 45.
117 Ibid s 52.

parties. If it becomes necessary to enforce the determination, action must be taken in the Federal Court or the Federal Magistrates Court.[118]

Public Interest Determinations

3.80 The Privacy Commissioner has the power to make Public Interest Determinations (PID) and Temporary Public Interest Determinations (TPID) that exempt certain acts and practices from the operation of the Act that would otherwise be a breach of the IPPs or NPPs.[119] 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.

3.81 The Privacy Commissioner has made nine PIDs to date. For example, PID 9 together with PID 9A, issued in October 2002, allow health service providers to collect health information from health consumers about third parties without the consent of the third party in the following circumstances:

- the collection of the third party's information is necessary for health service providers to provide a health service directly to the consumer; and

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

3.82 These PIDs were issued to meet the concern that the common practice of collecting family medical history information from patients in the course of delivering a health service was in breach of the *Privacy Act*.

3.83 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.[120]

Privacy Advisory Committee

3.84 The *Privacy Act* provides for the establishment of a Privacy Advisory Committee (Advisory Committee) made up of the Privacy Commissioner and not more than six other members.[121] The Act requires that members of the Advisory Committee have a range of expertise, for example, in industry or public administration, the trade

---

118 Ibid s 55A.

119 Ibid ss 72, 80A and 80B.

120 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 Interpretation Act* are to be legislative instruments for the purposes of the *Legislative Instruments Act*.

121 Ibid s 82. The Privacy Advisory Committee is discussed further in Ch 6.

union movement, electronic data processing, social welfare and civil liberties. The current members of the Advisory Committee are Mr Peter Coroneos, Chief Executive Officer, Internet Industry Association; Associate Professor John M O'Brien, School of Organisation and Management, University of New South Wales; Ms Suzanne Pigdon, former Manager Privacy, Coles Myer Ltd; Dr William Pring, Director of Consultation-Liaison, Psychiatry Services Box Hill Hospital; and Ms Joan Sheedy, Assistant Secretary, Information Law Branch, Attorney-General's Department.

3.85 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.[122]

122 Ibid s 83.

4. Examination of the Privacy Principles

Contents

Introduction

4.1 The privacy principles set out in the *Privacy Act 1988* (Cth) focus solely on the protection of personal information. The principles do not cover other areas of privacy such as bodily privacy, privacy from surveillance, or communications privacy.

4.2 This chapter considers a range of issues relating to privacy principles that regulate each stage of the information cycle beginning with the initial collection of personal information and ending with its erasure, disposal or similar mechanism. Intermediate stages in the cycle include the use, disclosure, storage, correction, retention of, and access to, personal information. The chapter examines the two sets of principles in the *Privacy Act* that apply to the public and private sectors respectively, and surveys information privacy principles at the international level, and in other jurisdictions—both within Australia and overseas.

4.3 Among the issues canvassed are: whether it is appropriate to maintain the existing framework of a separate set of privacy principles for the public and private sectors or whether there should be a single set of core principles; and whether there are specific areas of regulation, or particular types of personal information, that warrant specialised principles. Other issues are: determining the content of privacy information principles; whether these principles should be detailed or expressed at a high-level; and whether the model of principles to be adopted should aim to achieve a minimum or maximum level of privacy protection or adopt a best practice approach. Ascertaining the relative importance of the interests that the principles seek to protect and balance will be pivotal in determining how to resolve many of these issues during the course of the Inquiry.

OECD Guidelines

4.4 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 Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) set out in the *Privacy Act*.

4.5 The OECD Guidelines were adopted by the OECD Council on 23 September 1980. The impetus to the formulation of the Guidelines 'was the fear that [the member countries of the OECD] would introduce incompatible and conflicting laws for the defence of privacy in the newly established databases of the interlinked information technologies'.[1] The OECD Guidelines have been influential in shaping many data protection laws. They attempt to balance the protection of privacy and individual liberties with the advancement of the free flow of personal data—accepting certain restrictions to free transborder flow of personal data but seeking to reduce the need for

1 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 25.

such restrictions.[2] The Guidelines were developed to harmonise national privacy legislation, and while upholding human rights, simultaneously prevent interruptions in international flow of data.[3]

4.6 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'.[4] The Guidelines state that they only represent 'minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties'.[5] However, the OECD Guidelines also provide that member countries should not develop laws and policies in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.[6]

4.7 Part Two of the OECD Guidelines sets out eight basic principles of national application, namely, collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability.[7]

4.8 The OECD Guidelines are general in their application, although the Explanatory Memorandum notes that a question arose whether the Guidelines should be structured to deal with different types of data or activities, and expresses the view that 'it is probably not possible to identify a set of data which are universally regarded as being sensitive'.[8] The Explanatory Memorandum also notes the following key issue, which arises when considering the content of national privacy principles:

> 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 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.[9]

---

2 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [25].

3 Ibid, preface.

4 Ibid, Guideline 2.

5 Ibid, Guideline 6.

6 Ibid, Guideline 18.

7 See Ibid, Guidelines 7–14. These Guidelines are set out in full in Ch 1. The IPPs and NPPs, discussed below, do not contain an 'accountability' principle. However, 'accountability' provisions are found in the *Privacy Act 1988* (Cth), for example, provisions for investigations of complaints regarding privacy breaches. See Ch 6 which discusses the powers of the OPC.

8 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19(a)].

9 Ibid, Explanatory Memorandum, [19 (e)]. See also [50].

4.9 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 not sufficiently flexible to accommodate the extensive changes that have taken place since they were first promulgated.[10] He has stated that the OECD Guidelines reflect assumptions about the future development of information technology, which are now seen to be limited.[11] Justice Michael Kirby, who chaired the OECD Expert Group on Privacy, has stated:

> 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.[12]

4.10 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'.[13] 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).

4.11 The OECD Security Guidelines contain nine information systems security principles namely: awareness; responsibility; response; ethics; democracy; risk assessment; security design and implementation; security management; and reassessment.[14] 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 enhance security'[15] and the 'response' principle provides that 'participants should act in a timely and cooperative manner to prevent, detect and respond to security incidents'.[16]

---

10 J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part II' (1997) 3 *Privacy Law & Policy Reporter* 196, 199.

11 See J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part I' (1996) 3 *Privacy Law & Policy Reporter* 143, 144.

12 M Kirby, 'Privacy Protection, a New Beginning: OECD Principles 20 years on' (1999) 6 *Privacy Law & Policy Reporter* 25, 27. Ch 11 raises the issue of whether the *Privacy Act* should be technologically neutral.

13 See Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems* (1992).

14 See Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002).

15 Ibid, Principle 1.

16 Ibid, Principle 3.

Information Privacy Principles

4.12 While the OECD Guidelines apply to personal data in both the public and private sectors, there are separate sets of privacy principles in the *Privacy Act* applying to the two sectors. The IPPs cover the public sector and the NPPs cover the private sector. The issue arises whether it is appropriate to retain two sets of principles in the Act. To examine this issue properly, it is necessary to address and compare the content of each of the IPPs and NPPs

4.13 Section 14 of the *Privacy Act* sets out 11 IPPs. They regulate the collection, storage, use and disclosure of an individual's personal information, and provide for individuals to access and correct their personal information. The principles apply to personal information handled by Commonwealth and ACT government agencies.[17] The Privacy Commissioner has issued a series of guidelines on the interpretation of the principles.[18] 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.[19]

4.14 The 11 IPPs are addressed below. Some issues relating to the IPPs arise as a result of comparing their content with that of the NPPs. Accordingly, questions in relation to particular IPPs appear at the end of the discussion of the corresponding NPPs.

Principle 1: Manner and purpose of collection of personal information

4.15 IPP 1 provides that personal information shall not be collected by a 'collector' for inclusion in a 'record' or in a 'generally available publication'[20] unless: (a) the purpose for which the information is collected is lawful and directly related to a

---

17 See *Privacy Act 1988* (Cth) ss 13(a), 16. 'Agency' is defined extensively in *Privacy Act 1988* (Cth) s 6 and includes: a Minister; a Department; a body established for a public purpose; a federal court; and the Australian Federal Police.

18 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 Ch 6.

19 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).

20 *Privacy Act 1988* (Cth) s 6 defines 'record' and 'generally available publication'. Those definitions are discussed in Ch 3.

function or activity of the collector, and (b) the collection of the information is necessary or directly related to that purpose. In addition, personal information is not to be collected by unlawful or unfair means.

4.16 This principle applies to collection of information by whatever means, including solicitation from the individual concerned or from another source, or passive receipt of unsolicited information, for example, Ministerial letters and tip-offs by informers.[21]

4.17 Section 9 of the *Privacy Act* sets out who is to be treated as a 'collector' for the purposes of the Act. It includes an 'agency' that collects personal information. Where an individual collects information in the course of the person's employment by an agency or as a member of the Australian Federal Police (AFP) in the performance of duties as such a member, the agency or the AFP is considered to be the collector.

4.18 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.[22]

Principle 2: Solicitation of personal information from individual concerned

4.19 IPP 2 provides that where a collector solicits personal information directly from the individual concerned for inclusion in a record or in a generally available publication, the collector must take reasonable steps to ensure that before the information is collected, or if that is not practicable, as soon as practicable 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 collector's usual practice to disclose or pass on personal information of the kind collected.

4.20 The Explanatory Memorandum notes that there would be circumstances in which a collector 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.[23]

---

21 Explanatory Memorandum, Privacy Bill 1988 (Cth), [59].

22 Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 1–3: Advice to Agencies about Collecting Personal Information* (1994).

23 See Explanatory Memorandum, Privacy Bill 1988 (Cth), [61].

Principle 3: Solicitation of personal information generally

4.21 IPP 3 provides that where a collector solicits personal information for inclusion in a record or in a generally available publication, the collector must take reasonable steps to ensure that, having regard to the purpose for which the information is collected:

- the information collected is relevant to that purpose and is up-to-date and complete; and
- the collection does not intrude to an unreasonable extent upon the individual's personal affairs.

4.22 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 collector.[24]

Issues concerning unsolicited information

4.23 Agencies receive unsolicited material. In the area of community services, for example, unsolicited personal information is received by agencies concerning domestic violence or abuse. The issue arises whether any particular information privacy principles, apart from IPP 1,[25] should apply when an agency receives unsolicited information which it intends to include in a record or a generally available publication. The ALRC is interested in views on this issue.

Principle 4: Storage and security of personal information

4.24 IPP 4 provides that a record-keeper who has possession or control of a record that contains personal information shall 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.

---

24 Ibid, [63].

25 As noted above IPP 1 applies to unsolicited information: Ibid [59].

4.25 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.[26]

Principle 5: Information relating to records kept by record-keeper

4.26 IPP 5 provides that a record-keeper who has possession or control of records that contain personal information is to 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.

4.27 A record-keeper has to give a person information unless it is required or authorised not to do so by a Commonwealth law that provides for access to documents.[27] 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.

Principle 6: Access to records containing personal information

4.28 IPP 6 provides that an individual is entitled to have access to a record that contains his or her personal information and that 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 provisions of Commonwealth law providing for access by persons to documents.

4.29 Unlike the Individual Participation Principle in the OECD Guidelines, IPP 6 is silent on the timing and form of, and charges relating to, access. The mechanism for accessing records held by the government is located in the *Freedom of Information Act*

---

26 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).

27 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).

1982 (Cth) (FOI Act).[28] Amendments were made to the FOI Act at the time of passage of the *Privacy Act* to support access to personal information.[29]

Principle 7: Alteration of records containing personal information

4.30 IPP 7 provides that a record-keeper who has possession or control of a record that contains personal information is to take reasonable steps (by way of making appropriate corrections, deletions and additions) to ensure that the record is accurate and is, having regard to the purpose for which the information was collected or is to be used or any directly related purpose, 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 provisions of a 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.

4.31 In most cases, an application by an individual for the amendment of personal information initially should be made under the FOI Act in order to avoid unnecessary administrative duplication.[30] The right to amendment under the *Privacy Act,* however, is broader than the corresponding right in the FOI Act. Thus, there are circumstances in which an application for amendment will need to be dealt with from the outset under IPP 7, rather than pursuant to the FOI Act. These include: where the amendment sought is on the ground 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.[31]

Principle 8: Record-keeper to check accuracy

4.32 IPP 8 provides that a record-keeper who has possession or control of a record containing personal information is not to use that information without taking reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used, the information is accurate, up-to-date and complete.

---

28 The interaction between the *Privacy Act* and the FOI Act regarding access and amendment rights is discussed further in Ch 7.

29 See Australian Government Attorney-General's Department, *Freedom of Information Memorandum 93: FOI and the Privacy Act* (1992).

30 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.

31 See Ibid, 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].

4.33 Section 6 of the *Privacy Act* provides that 'use in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication'.

Principle 9: Personal information to be used only for relevant purposes

4.34 This principle provides that a record-keeper who has possession or control of a document that contains personal information shall not use the information except for a purpose to which the information is relevant.

Principle 10: Limits on use of personal information

4.35 IPP 10 provides that a record-keeper who has possession or control of a record that contains personal information must not use that information for any purpose other than that for which it obtained the information unless:

- the individual the information is about consents to the use;[32]
- the record-keeper believes on reasonable grounds that the use is necessary to prevent or lessen a serious and imminent threat to a person's life or health;[33]
- the use is authorised or required by law;
- the use is reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty or to protect the public revenue; or
- the use is directly related to the purpose for which the information was obtained.

4.36 Where the personal information is used for the enforcement of the criminal law or a law imposing a pecuniary penalty or to protect the public revenue, the record-keeper is to include in the record containing that information a note of that use.

4.37 IPP 10 deals only with the use of personal information, whereas the Use Limitation Principle in the OECD Guidelines deals simultaneously with use and disclosure. One criticism raised in consultation was the fact that use and disclosure are dealt with separately in the IPPs, and that disclosure could be cast as use. It was suggested that it would be more practical for the issues to be dealt with together in one principle.[34]

---

32 'Consent' can be express or implied. See *Privacy Act 1988* (Cth) s 6.

33 The 'life' and 'health' exceptions should only be used in emergency situations and not for routine disclosures. See 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 *Privacy Legislation Amendment Act 2006* (Cth) amends NPP 2.1—the counterpart to IPPs 10(1)(b) and 11(1)(c)—by allowing organisations to use or disclose genetic information to genetic relatives of an individual without requiring that the relevant threat be 'imminent'.

34 A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

Principle 11: Limits on disclosure of personal information

4.38 IPP 11 provides that a record-keeper who has possession or control of a record that contains personal information must not disclose the information to anyone other than the individual to whom the information relates unless:

- 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 person, body or agency;
- the individual the information is about consents to the disclosure;
- the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to a person's life or health;
- the disclosure is authorised or required by law;[35] or
- the disclosure is reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty or to protect the public revenue.

4.39 Where the personal information is disclosed for the last reason, the record-keeper is to include in the record containing that information a note of the disclosure. IPP 11 also provides that the person, body or agency to whom personal information is disclosed is not to use or disclose the information for a purpose other than the purpose for which the information was disclosed.

Issues relating to IPP 11

4.40 Agencies' concerns to protect the privacy of individuals can make them unwilling to share or disclose personal information, and there is a concern that, at times, this can be a block to the protection and care of vulnerable people.[36] The Community Services Ministers' Advisory Council expressed concern that it was too high a threshold to have to establish that a threat to a person's life or health was both 'serious and imminent' in order to justify a disclosure. It submitted:

> 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.[37]

---

35 Examples of provisions that authorise or require disclosure are discussed in Ch 7.
36 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.
37 Ibid.

4.41 Another issue is the operation of IPP 11 in the context of disaster recovery and consular crisis management. The Department of Foreign Affairs and Trade (DFAT), in its submission to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (the Senate Committee privacy inquiry), noted its consular obligations to assist Australians overseas in times of emergency. It identified two key privacy impediments to responding to the emergencies of the terrorist attacks in the United States (US) on 11 September 2001, the Bali bombings of 2002 and the Boxing Day tsunami of 2004:

- DFAT's ability to access personal information held by other bodies to assist in its location, identification and assistance efforts;[38] and
- DFAT's ability to provide personal information to other bodies directly involved in the crisis response.[39]

4.42 DFAT submitted that while it might be able to provide personal information to other agencies directly involved in the crisis response, not all cases where disclosure was sought could be classified as posing a 'serious and imminent' threat to life or health.[40]

4.43 A related issue is how to ascertain whether there is an emergency that would justify the disclosure of personal information by agencies. DFAT expressed the view that it was preferable to avoid ministerial declarations of emergencies.[41] The Australian Government's recently proposed model to ascertain the existence of an emergency is discussed below, and other possible mechanisms are raised below in relation to NPP 2.

4.44 DFAT also identified an impediment regarding its ability to provide personal information to other bodies requesting the information to ensure that inappropriate action is 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.[42]

4.45 Community service agencies also play an important part in disaster recovery. The sharing and disclosure of personal information between agencies is often a necessary part of this process. The sharing of personal information between agencies and organisations, particularly non-government organisations, may also be desirable in this context. However, while IPP 11 appears to allow the sharing of information with

---

38 An example of such information is up-to-date contact and next of kin details from the Health Insurance Commission. 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.

39 Ibid.

40 Ibid.

41 Australian Government Department of Foreign Affairs and Trade, *Consultation PC 10*, Canberra, 29 March 2006.

42 Department of Foreign Affairs and Trade, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 8 March 2005.

regard to an immediate disaster response, the Community Services Ministers' Advisory Council has submitted that the position in relation to disaster recovery is less clear.[43]

4.46 Canadian privacy legislation 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.[44] Such an approach would allow for the sharing of information in emergencies and in disaster recoveries. In this regard, the *Privacy Act* empowers the Privacy Commissioner to make a temporary public interest determination.[45]

4.47 On 13 September 2006, the Australian Government introduced the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Cth) into Parliament. The Bill would insert a new Part VIA in the *Privacy Act* to enhance information exchange between Australian Government agencies, state and territory authorities, organisations, non-government organisations and others, in an emergency or disaster situation. Part VIA would 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. Part VIA would be triggered upon the making of a declaration by the Prime Minister or the Attorney-General.[46]

4.48 Another issue that arises in relation to IPP 11 is that it does not appear to accommodate disclosure of personal information to the police to assist them in policing activities undertaken in the public interest that do not involve the enforcement of a criminal law. So, for example, disclosure of information to the police so that they may assist in emergencies, for example by identifying victims of disasters, or so that they may ascertain whether a missing person is in fact missing, are scenarios which do not appear to be always accommodated by the privacy principles.[47]

4.49 Unlike NPP 2.1 (discussed below), which contains a note that the principle is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions, IPP 11 does not contain such a note.

4.50 The Salvation Army noted that the disclosure limitations under the *Privacy Act* frustrated its efforts to assist in the search efforts of persons separated by New South

---

43 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

44 *Privacy Act* RS 1985, c P-21 (Canada) s 8(2).

45 *Privacy Act 1988* (Cth) s 80A. Public interest determinations are discussed in Chs 3 and 6.

46 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).

47 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.

Wales Government intervention and in carrying out its work in relation to the Army's world-wide Family Tracing Service.[48]

National Privacy Principles

4.51 In the Second Reading Speech of the Privacy Amendment (Private Sector) Bill 2000, the then Attorney-General, Daryl Williams stated:

> The aim of this bill is to encourage private sector organisations and industries which handle personal information to develop privacy codes of practice. Where an organisation does not put a privacy code in place, the national privacy principles will apply. The national privacy principles will also provide the benchmark for industry codes.[49]

4.52 Schedule 3 to the *Privacy Act* sets out 10 NPPs.[50] These principles are addressed below. Some of the issues concerning the NPPs are the subject of recommendations made by the Office of the Privacy Commissioner (OPC) in its review of the private sector provisions of the *Privacy Act* (the OPC Review).[51] The Senate Committee privacy inquiry endorsed the findings and recommendations of the OPC Review and recommended that the Australian Government implement those recommendations as a matter of priority.[52] However, the Senate Committee privacy inquiry also expressed the view that the OPC Review could have gone further in its recommendations and disagreed with the OPC Review's conclusion that the private sector provisions are 'working well'.[53]

4.53 The ALRC invites views in relation to the particular issues set out below in respect of which the OPC Review has made recommendations, as well as views in relation to the appropriateness and efficacy of the OPC Review's response to those issues. As will be evident from the discussion below, a number of recommendations made in the OPC Review are directed to the OPC itself, calling on it to develop further guidance in particular areas. At the time of writing, the OPC had not published guidelines pursuant to recommendations made in the OPC Review, however the OPC recently received additional resources and has indicated an intention to proceed to develop the guidelines.

---

48 See Salvation Army, *Submission PR 15,* 2 June 2006.

49 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15749–15750.

50 An organisation that is subject to the credit reporting provisions under pt IIIA and the Credit Reporting Code of Conduct must also comply with the NPPs or an approved privacy code. See *Privacy Act 1988* (Cth) s 16A(3), (4). Credit reporting will be the subject of a separate Issues Paper.

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).

52 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.27] and Rec 10.

53 Ibid, [7.27].

Principle 1: Collection

4.54 NPP 1 provides that an organisation[54] must:

- not collect information unless it is necessary for one or more of its functions or activities;
- collect personal information only by lawful and fair means and not in an unreasonably intrusive manner;
- at or before the time of collection of personal information from the individual concerned (or if that is not practicable, as soon as possible after), take reasonable steps to ensure that the individual is aware of: the identity of the organisation and how to contact it; 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 that requires the particular information to be collected; and the main consequences for the individual if the information is not provided;[55]
- collect information about an individual only from that individual if it is reasonable and practicable to do so; and
- if it collects personal information from someone other than the individual concerned, take 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 the life or health of any individual.[56]

4.55 The obligations in relation to the collection of information by organisations generally depend on collection of that information for inclusion in a record or generally available publication.[57]

Gaps in the IPPs

4.56 A comparison of NPP 1 and IPPs 1–3 (which deal with collection) reveals that although they share some common ground, there are a number of potential gaps in the IPPs in relation to collection. NPP 1, unlike IPPs 1–3, imposes an obligation on an organisation, where reasonable and practicable to do so, to collect information about an individual *only* from that individual. The issue arises whether it is appropriate to

---

54 'Organisation' is defined in *Privacy Act 1988* (Cth) s 6C. The definition is addressed in Chs 3 and 5.
55 Ibid sch 3, NPP 1.3.
56 Ibid sch 3, NPP 1.5.
57 See Ibid s 16B; Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [328]. This does not apply to pt III divs 3 and 4 (tax file numbers and credit information) and pt IIIA (credit reporting).

impose an obligation on agencies to collect information only from the individual concerned. There is precedent for such a provision. The New South Wales privacy legislation imposes such an obligation on a public sector agency unless the individual has authorised collection from someone else or, where the information relates to a person under 16 years of age, the information has been provided by a parent or guardian of the person.[58] The US privacy legislation imposes an obligation on 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.[59]

4.57 Similarly, Canadian privacy legislation requires 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.[60]

4.58 In addition, IPP 2, unlike NPP 1, does not contain an express requirement that an individual be made aware of the collector's identity and contact details nor does it require that the individual concerned be made aware of the fact that he or she is able to gain access to the information and of the main consequences of not providing the information.[61]

Gaps in the IPPs and NPPs

4.59 Neither the IPPs or NPPs require an agency or organisation to notify an individual of the source of personal information it has collected where that information was not collected directly from the individual. The ALRC is interested in views as to whether such an obligation should be imposed on agencies and organisations. In this regard, German information privacy legislation provides that a data subject should be provided with information about stored data concerning him or her including any reference to their origin.[62]

4.60 There are no requirements in the NPPs or IPPs relating to the provision of information to individuals at the time of collection of personal information about various avenues of complaint available. The ALRC is interested in hearing whether such an obligation should be imposed on agencies and organisations. The OPC Review recommended that the Australian Government consider amending NPP 1.3 to require

---

58 *Privacy and Personal Information Protection Act 1998* (NSW) s 9.
59 See *Privacy Act 1974* 5 USC § 552a (US).
60 See *Privacy Act* RS 1985, c P-21 (Canada) s 5(1). See also *Privacy Act 1993* (NZ) s 6, IPP 2 and *Federal Data Protection Act 1990* (Germany) s 4(2).
61 Compare *Privacy Act 1993* (NZ) s 6, Principles 3(1)(d), (f), (g).
62 See *Federal Data Protection Act 1990* (Germany) ss 19(1), 34(1).

organisations to inform individuals about their avenues of complaint to the organisation, the Privacy Commissioner, and, where relevant, the code adjudicator.[63]

Issues relating to NPP 1

4.61 NPP 1 does not distinguish between the obligations on an organisation in respect of solicited and unsolicited information, although it does separately address personal information obtained directly from the individual concerned, and information collected from 'someone else'.[64] The issue arises whether any particular information privacy principles should apply when an organisation receives unsolicited information which it intends to include in a record or a generally available publication. A related issue is whether privacy principles should be amended to accommodate the passive 'accretion' of personal information by organisations—and agencies—through the application of new technologies.[65]

4.62 There is a lack of clarity in the wording of NPP 1.5 to the extent that it refers to an organisation's obligations 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.[66] The OPC recommended that consideration be given to amending NPP 1.5 to make it clear that an organisation's obligations under that principle apply when collecting personal information indirectly, from any source.[67] An Information Sheet developed by the OPC interprets NPP 1.5 as applying when an organisation collects personal information from publicly available sources, as well as when it collects it from other individuals, or organisations and agencies.[68] The OPC noted that the information sheet has gained widespread acceptance.[69]

4.63 The ALRC is interested in views in relation to the efficacy of the OPC's recommendation that NPP 1.5 should be amended to make it clear that the obligations imposed on an organisation when collecting personal information apply irrespective of the source of the information, and whether this recommendation should extend to unsolicited personal information that an organisation intends to include in a record or

---

63 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.

64 See *Privacy Act 1988* (Cth) sch 3, NPPs 1.4, 1.5.

65 Developing technologies are discussed in Ch 11. See, in particular, Question 11–3.

66 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 the availability of publicly available sources in an electronic form are discussed in Ch 11.

67 Ibid, Rec 76.

68 Office of the Federal Privacy Commissioner, *Privacy and Personal Information That is Publicly Available*, Information Sheet 17 (2003).

69 Australian Government Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 262.

generally available publication. The ALRC is also interested in views on the issue of whether this approach could be extended to the collection of personal information by agencies.

4.64 Specific issues arise relating to the extent of the obligation of an organisation to provide information to an individual at the time of collection. The issue of whether short form privacy notices should be provided for in the *Privacy Act* is raised in the discussion below on the openness principle in NPP 5. One issue is that under NPP 1.3 an organisation is only required to ensure that an individual is aware of the 'organisations' to which it usually discloses information of that kind. However, 'organisation' has a restricted meaning for the purposes of the *Privacy Act*, excluding, for example, political parties and state or territory agencies. Therefore on a strict interpretation of the principle, an organisation would not have to tell an individual about likely disclosures to the Australian Government, or to state and local government agencies. As noted by the OPC, this appears to be inconsistent with the policy intent of the legislation because the Explanatory Memorandum envisages disclosure to state government licensing authorities, which do not fall within the definition of 'organisation'.[70]

4.65 The OPC recommended 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.[71] The ALRC is interested in views on this issue and on the OPC's recommendation.

4.66 There is a degree of uncertainty as to whether or not the requirement under NPP 1.3 and NPP 1.5 for an organisation to take 'reasonable steps' to ensure that the person or other body from whom the organisation collects the information is aware of certain specified matters, would allow an organisation to determine that in some circumstances taking no steps is reasonable. For example, the OPC 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 has been collected incidentally, or in many circumstances where the information is collected from a public source.[72]

4.67 The OPC recommended that the legislation make it clear that that there are situations in which the reasonable steps an organisation might take to provide notice to

---

70 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 259; Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [3.34].

71 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.

72 Ibid, 260.

an individual may equate to no steps.[73] Professor Roger Clarke has expressed a similar view.[74]

4.68 The Australian Privacy Foundation submitted to the Senate Committee privacy inquiry that the NPPs should provide that collection should be limited to purposes that a reasonable person would consider appropriate in the circumstances.[75] The 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 stating that while it would enable an individual to challenge the collection of personal information, in practice it would be difficult to implement.[76] Canadian privacy 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'.[77] The ALRC is interested in views about the introduction of a similar test in the *Privacy Act*.

Question 4–1 Are the obligations imposed on **organisations** at the time of collection of personal information adequate and appropriate? For example, should an organisation also be required to make an individual aware of (a) the types of people, bodies or agencies to whom the organisation usually discloses information of that kind; (b) the various avenues of complaint available; and (c) the source of the information, where it has not been collected directly from the individual?

Question 4–2 Should NPP 1 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 aware of specified matters relating to the collection of personal information?

73 Ibid, Rec 75

74 R Clarke, 'Serious Flaws in the National Privacy Principles' (1998) 4 *Privacy Law & Policy Reporter* 176, 179.

75 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.

76 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 91.

77 *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) s 5(3). See also s 3.

Question 4–3 Are the obligations imposed on **agencies** at the time of collection of personal information adequate and appropriate? In particular, should agencies also be subject to a general requirement that where reasonable and practicable, they should collect information about an individual only from the individual concerned? Should agencies also be required to notify an individual of his or her rights of access to the information, the consequences of not providing the information, the various avenues of complaint available, and the source of the information, where it has not been collected directly from the individual?

Question 4–4 Should any obligations attach to an agency or organisation which receives unsolicited personal information that it intends to include in a record or generally available publication? If so, what obligations should be imposed?

Question 4–5 Should the obligations imposed on an organisation or agency at or soon after collection apply irrespective of the source of personal information?

Principle 2: Use and disclosure

4.69 NPP 2.1 provides that an organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection except in particular designated circumstances. Those circumstances are:

- where 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[78]—**and** the individual would reasonably expect the organisation to use or disclose the information for the secondary purpose;[79]
- the individual has consented to the use or disclosure;
- if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing, but only where a number of specified criteria are met. These include that: it is impracticable for the organisation to seek the individual's consent for that particular use; no request has been made by an individual not to receive direct marketing material; the organisation draws to the individual's attention or prominently displays a notice

78 Issues that arise in ascertaining the primary purpose of collecting health information are discussed in Ch 8.

79 The definition of 'sensitive information' is set out in Ch 3.

that he or she may express a wish to not receive further direct marketing communications; and each written direct marketing communication sets out the organisation's contact details, including electronic contact details if the communication is by electronic means;[80]

- if the information is health information[81] and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health and safety, but only where a number of specified criteria are met. These include: that 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 Privacy Commissioner; and in the case of disclosure, the organisation reasonably believes the recipient will not disclose the health information;

- 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;[82]

- the organisation has reason to suspect past, current or prospective unlawful activity and uses or discloses the personal information as a necessary part of its investigation or in reporting its concerns to relevant authorities;

- the use or disclosure is required or authorised by law; or

- the organisation reasonably believes that the use or disclosure is reasonably necessary for specified functions of an enforcement body. These include: the prevention, detection, investigation, prosecution or punishment of criminal offences, or breaches of a law imposing a penalty or sanction; the enforcement of laws relating to the confiscation of proceeds of crime; the protection of the public revenue; or the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct.[83]

4.70 NPP 2.4 specifies when an organisation that provides a health service to an individual can disclose that information to a person who is 'responsible' for the individual.[84] Disclosure may occur if:

---

80 See *Privacy Act 1988* (Cth) sch 3, NPP 2.1(c).

81 Health information is sensitive information for the purposes of the Act. See Ibid s 6.

82 The *Privacy Legislation Amendment Act 2006* (Cth) allows the disclosure of genetic information about an individual to genetic relatives of that individual without requiring that the relevant threat be 'imminent'.

83 An organisation must make a written note of any use or disclosure under this limb: *Privacy Act 1988* (Cth) sch 3, NPP 2.2.

84 Under Ibid sch 3, NPP 2.5 a 'responsible' person includes specified family members.

- the individual is physically or legally incapable of giving consent to the disclosure or physically cannot communicate consent to the disclosure;

- the natural person (the carer) providing the health service for the organisation is satisfied that either the disclosure is necessary to provide care or treatment, or the disclosure is made for compassionate reasons;

- the disclosure is not contrary to any previously expressed wish of the individual; and

- the disclosure is limited to the extent reasonable and necessary for the purpose of disclosure.

Comparison with IPPs and state legislation

4.71 Unlike the IPPs,[85] NPP 2 deals simulantaneously with the use and disclosure of personal information. In this regard, it is consistent with the approach taken in the Use Limitation Principle in the OECD Guidelines.[86]

4.72 Also, unlike the IPPs, NPP 2 expressly uses the language of 'primary purpose'[87] and 'secondary purpose' of collection. 'Secondary purpose' is defined as any purpose other than the primary purpose of collection. IPP 10 refers to constraints on using personal information obtained for a *particular purpose* for *any other purpose*.

4.73 While NPP 2 allows use and disclosure of personal information where the secondary purpose is related to the primary purpose of collection, it imposes a higher test where the personal information is sensitive, requiring that there be a 'direct' relation. The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states:

> The sensitivities associated with the use or disclosure of sensitive information mean that a stronger connection should be demonstrated between the primary purpose for collection and the secondary purpose.[88]

4.74 NPP 2 does not, however, go as far as IPP 10 which requires a direct relation in respect of the purpose for which *any* personal information is used and the particular purpose for which it was obtained. The IPPs do not create a separate test for 'sensitive information'—they apply the stricter test to all personal information. However, unlike NPP 2, IPP 10 does not impose the additional 'reasonable expectation' test—that is,

---

85 Ibid s 14, IPPs 10 and 11 deal separately with use and disclosure.

86 See Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 9.

87 'Primary purpose' is not defined but appears to relate to the functions or activities of an organisation. See *Privacy Act 1988* (Cth) sch 3, NPP 1.1.

88 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [342].

that in order to use personal information for a secondary purpose, the individual must reasonably expect the agency to use the information for that other purpose.

4.75 While there are some similarities between NPP 2 and IPPs 10 and 11—for example both have the following exceptions: consent by the individual, where use or disclosure is required or authorised by law, and where there is a serious and imminent threat to the life or health of an individual—there are also some key differences. These differences include that NPP 2 includes exceptions for: the safety of an individual, public health and public safety; the preparation for, or conduct of, court or tribunal proceedings; prevention and investigation of 'seriously improper conduct'; direct marketing where specified criteria are met, and for the use or disclosure of health information for research or statistics relevant to public health and safety where specified criteria are met. In addition, unlike the IPPs, NPP 2 contains notes which make it clear 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.[89]

4.76 Unlike both the NPPs and the IPPs, Victorian and Tasmanian privacy legislation also allows for the use or disclosure of personal information where the relevant body believes that it is necessary to prevent a serious and imminent threat to an individual's welfare.[90] Victorian privacy legislation also permits a public sector body to use or disclose personal information where it reasonably believes it is necessary to prevent or lessen a serious threat to public welfare.[91]

Issues relating to NPP 2

4.77 The limitations of NPP 2 in dealing with the disclosure of non-health information concerning adults with a decision-making disability are raised in Chapter 9. That chapter also discusses issues relating to the use and disclosure of the personal information of children and young people.

Dealing with natural disasters or other emergencies

4.78 The exceptions in NPP 2 do not cater adequately for the disclosure of personal information by organisations to government departments and other relevant bodies to deal with emergencies and disaster recoveries which may not involve a relevant threat that is 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, DFAT may need to ascertain whether a particular individual was in the affected location at the

89 See *Privacy Act 1988* (Cth) sch 3, NPP 2, Notes1–3.

90 *Information Privacy Act 2000* (Vic) sch 1, IPP 2.1(d)(i); *Personal Information Protection Act 2004* (Tas) sch 1, Personal Information Protection Principle (PIPP) 2(1)(d)(i).

91 *Information Privacy Act 2000* (Vic) sch 1, IPP 2.1(d)(ii).

time of the disaster for identification purposes and to provide information to family members. DFAT stated that travel agents who have information relating to the whereabouts of individuals can be reluctant to release such information because they are uncertain of the scope of the exceptions in the *Privacy Act*.[92] In its submission to the Senate Committee privacy inquiry DFAT stated:

> To meet our consular obligations, it would be useful to be able to access the records of airline and travel agents, regarding the travel plans, hotel reservations, and therefore general whereabouts, of Australians overseas.[93]

4.79 There is also an issue about individuals being able to obtain from organisations in time of emergency information about family members and friends. For example, in an attempt to locate missing family and friends after the 2004 tsunami, many Australians contacted airlines to ascertain whether the missing had continued to fly after the tsunami hit.[94] The OPC Review raised the possibility that NPP 2 could be amended to deal with emergencies by allowing for disclosure based on compassionate grounds to a 'person responsible' where the individual is unable to consent to the disclosure and is not contrary to any wish expressed by the individual.[95] Under NPP 2.4 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 national emergency. The OPC recommended that the definition should be extended to include a person nominated by the family to act on its behalf.[96]

4.80 As mentioned above, an issue also arises as to how to define an emergency, and whether there is a need for a mechanism to ascertain the existence of an emergency. Two possible models for determining the existence of an emergency were identified by the OPC Review and were the subject of recommendations. The OPC recommended that consideration be given to defining 'national emergencies' as 'incidents' determined by the Minister under s 23YUF of the *Crimes Act 1914* (Cth), and to amending the *Privacy Act* to enable the Privacy Commissioner to make a temporary public interest determination without requiring an application from an organisation.[97]

---

92 Australian Government Department of Foreign Affairs and Trade, *Consultation PC 10*, Canberra, 29 March 2006.

93 Department of Foreign Affairs and Trade, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 8 March 2005.

94 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 234.

95 See Ibid, 236; Rec 68.

96 See Ibid, Rec 68.

97 See Ibid, Rec 68; *Privacy Act 1988* (Cth) s 80A. Ch 6 discusses temporary public interest determinations. On 13 September 2006, the Australian Government introduced the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 (Cth) into Parliament, which makes special provision for the collection, use and disclosure of personal information in emergencies and disasters. See discussion above.

Law enforcement functions

4.81 There is also concern that the exceptions in NPP 2 do not cover disclosure of personal information to law enforcement authorities, and the use of the information by them, when undertaking functions that do not or may not involve a criminal offence or breach of the law, such as missing person investigations. 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.[98]

4.82 The OPC Review noted that the submissions did not generally call for a change to the NPPs in the law enforcement context, however, problems in applying the law in this area were identified.[99] For example, the AFP noted the reluctance of some organisations to provide personal information due to: ignorance of the fact that they were permitted to do so under the NPPs for law enforcement purposes; concerns about disclosures being detrimental to commercial interests; the costs of complying with a request for information; or 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 to understand better their obligations under the *Privacy Act*.[100]

4.83 In its submission to the Senate Committee privacy inquiry, however, the AFP noted that while education may have a role to play in raising awareness, it was unlikely to offer a complete solution. The AFP submitted that a legislative approach, such as empowering the AFP to issue a notice to produce, may be a possible solution.[101] The Senate Committee privacy inquiry supported the OPC's recommendation to develop practical guidance in this area, but considered that the Australian Government should also consider additional mechanisms to resolve the issue.[102] The ALRC is interested in views on this issue.

Notification of 'incidents' by insured professionals to insurers

4.84 There is a question 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

---

98 *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(1)(g)(vi).

99 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 223.

100 Ibid, Rec 65.

101 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.119], [5.121].

102 Ibid, [7.52].

committees', often comprising experts in the relevant profession, who advise insurers about making provision for possible future claims.

4.85 For example, a doctor may need to notify his or her insurer of an incident 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 disclosure of the patient's personal information is less clear. If the disclosure involves sensitive information, such as health information, NPP 2.1(a) requires that the purpose of advising in relation to indemnity be 'directly related' to the primary purpose of collection of the patient's information, 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 cases committees as a pre-condition to the provision of the health service;[103] 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.

4.86 The ALRC is interested in hearing 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.[104]

Logging disclosures

4.87 The ALRC's 1983 report *Privacy* (ALRC 22) refrained from recommending a general requirement that record-keepers keep a log of all uses and disclosures of personal information on the basis that the administrative costs associated with such a requirement were high. However, it suggested that the Human Rights Commission encourage record-keepers to adopt the practice of logging disclosures, at least in relation to disclosures that would represent a specially objectionable interference with individual privacy.[105]

4.88 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.[106] Professor Clarke has criticised NPP 2 because it does not require

103 Bundled consent is discussed below.
104 Public interest determinations are discussed in Ch 6.
105 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Vol 2, 197.
106 See *Privacy Act 1988* (Cth) sch 3, NPP 2.2.

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'.[107]

4.89 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 each Commonwealth agency 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.[108] The ALRC is interested in views on this issue.

Bundled consent

4.90 Bundled consent refers to the practice of bundling together consent to a wide range of uses and disclosures of personal information without giving individuals an opportunity to select to which uses and disclosures they agree. Bundled consent is often sought as part of the terms and conditions of a service.[109] Submissions from consumer groups to the OPC Review were highly critical of the practice, stating, for example, that it undermines the requirement that consent be meaningful, informed and freely given.[110] Similar sentiments were expressed in some submissions to the 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 disclosure, or when told that services would not be provided in the absence of consent.[111]

4.91 On the other hand, there may be legitimate circumstances in which organisations seek bundled consent from consumers. Submissions from the business sector—in particular the finance and telecommunications industries—to both the OPC Review and the Senate Committee privacy inquiry emphasised the necessity of seeking bundled consent in order to achieve business efficiency and to reduce costs to the

---

107 R Clarke, 'Serious Flaws in the National Privacy Principles' (1998) 4 *Privacy Law & Policy Reporter* 176, 177.

108 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.

109 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 82.

110 Ibid, 85.

111 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].

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.[112] Vodafone submitted to the OPC Review that unbundling consent would have negative outcomes for consumers and suppliers insofar as it would result in increased volume and frequency of communications.[113] Submissions from the finance industry emphasised that seeking a single consent for multiple uses of information, in an application for finance for example, 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.[114]

4.92 The OPC stated that it would develop guidelines on bundled consent.[115] The ALRC is interested in views relating to the practice of bundled consent, the manner in which bundled consent is obtained, and whether there is a need for legislative guidance in this area.

Direct marketing

4.93 Direct marketing involves the promotion and sale of goods and services directly to consumers. Direct marketers compile lists of consumer names and contact details from a wide variety of 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. For example, an individual may enter a competition to win prizes assuming that the primary purpose of the competition is to provide individuals with an opportunity to win prizes. In fact, the organisation's primary purpose in running the competition is often to collect personal information for direct marketing, and its secondary purpose is to award prizes to winning entrants.[116]

4.94 During the National Privacy Phone-In conducted by the ALRC on 1 and 2 June 2006, the majority 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 submissions also identified the practice of direct marketing as an area of concern.[117] Issues that arise

---

112 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]. Concerns relating to bundled consent in the context of credit reporting will be addressed in a separate Issues Paper.

113 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 86.

114 Ibid, 86.

115 Ibid, Rec 22.

116 Ibid, 95.

117 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.

from the practice of direct marketing and the application of the direct marketing principles were considered by the OPC Review.[118] Issues include: whether the *Privacy Act* should contain the assumption that personal information can be used for direct marketing; whether the criteria that need to be met in order to use personal information for the secondary purpose of direct marketing are sufficient—in particular whether consumers should be given the opportunity to 'opt in' to direct marketing instead of having the choice to 'opt out', and if an 'opt-out' model is preferred whether the Act should require organisations to comply with the 'opt-out' request within a specified time. Another issue is whether organisations should be required to advise individuals from where they acquired their personal information. The OPC recommended that the Australian Government should consider amending the *Privacy Act* to impose an obligation on organisations to comply with 'opt-out' requests within a specified time after receipt, and to require organisations to take reasonable steps, on request, to advise an individual where it acquired the individual's personal information.[119]

4.95 The Senate Committee privacy inquiry recommended that the ALRC's review of privacy laws consider the possibility of an 'opt-in' regime for direct marketing in line with the *Spam Act 2003* (Cth).[120] In this regard, art 14(b) of 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) provides for an 'opt-out' model.[121]

4.96 Legislative attempts to curtail specific types of direct marketing, namely telemarketing and spam, are discussed in Chapter 10. The *Do Not Call Register Act 2006* (Cth)—directed to telemarketing—adopts an 'opt-out' model; while the *Spam Act*—directed to email marketing—adopts an 'opt-in' model. This raises the issue of whether it is appropriate for privacy principles in the *Privacy Act* to attempt to prescribe a 'one size fits all' model for all types of direct marketing. It also raises the broader issue of whether the regulation of direct marketing should be dealt with by the privacy principles or by specific legislative provisions tailored to particular types of direct marketing.[122] One option, for example, may be for the *Privacy Act* to adopt an 'opt-out' model except where other legislation specifically allows for an 'opt-in' model. In other words, the privacy principles could aim to set a minimum standard only. The ALRC is interested in views on this issue.

---

118 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.

119 See Ibid, Recs 23, 24.

120 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 15.

121 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).

122 See Question 10–2.

Research involving non-health information

4.97 While NPP 2 allows for the use and disclosure of 'health' information for research purposes in certain circumstances it does not make any provision for the use and disclosure of non-health information for research purposes.

4.98 The OPC Review noted the need for an inquiry to ascertain the appropriate balance between facilitating research for public benefit and individual privacy.

> [R]esearchers … consider that the current balance between privacy and 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.[123]

4.99 The OPC recommended that the Australian Government consider whether there is a need to amend NPP 2 to permit the use and disclosure of personal information by organisations for research that does not involve health information.[124]

4.100 In this regard, Canadian privacy legislation allows organisations to use and disclose personal information where it is

> for statistical or scholarly study or research, purposes that cannot be achieved without [using or disclosing] the information, it is impracticable to obtain consent and the organisation informs the Commissioner of the [use or disclosure prior to the information being used or disclosed].[125]

4.101 The issue also arises whether the IPPs should also allow for use and disclosure of personal information for research purposes. For example, the privacy legislation of Victoria allows public sector bodies to use and disclose personal information (not just health information)

> if [it is] necessary for research, or the compilation or analysis of statistics, in the public interest, other than for publication in a form that identifies any particular individual
>
> (i) if it is impracticable for the organisation to seek the individual's consent before the use or disclosure; and
>
> (ii) in the case of disclosure—the organisation reasonably believes that the recipient of the information is not likely to disclose the information.[126]

4.102 The privacy legislation of Tasmania has a similar provision.[127] Canadian privacy legislation also allows government institutions to disclose personal information to any person or body for research or statistical purposes in specified circumstances.[128]

---

123 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

124 Ibid, Rec 60.

125 See *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) ss 7(2)(c); 7(3)(f).

126 *Information Privacy Act 2000* (Vic) sch 1 IPP 2(c).

4.103 The ALRC is interested in views on this issue.

Disclosure to remedy mistakes

4.104 Some stakeholders have expressed concern that where a mistake is made in processing an electronic or internet banking transaction and payment is made to an incorrect payee, banks refuse to disclose information about the recipient of those funds to enable recovery of the payment, on the basis that such disclosure is not permitted under the *Privacy Act*.[129] Link Market Services, a share registry, submitted:

> Link is provided with bank account details by shareholders. These can be misquoted or miskeyed and at the time of a dividend or other payment the money can be transferred into someone else's bank account mistakenly. When this occurs Link is unable to get access to the name or details of the person who mistakenly receives the money. The bank can follow up the individual on our behalf but this is not usually successful.[130]

4.105 This raises the question whether the *Privacy Act* should be amended to allow disclosure of personal information in order to remedy mistaken transactions in certain circumstances, for example, where a person or entity has been unjustly enriched as a result of that transaction. The ALRC is interested in views on this issue.

Due diligence

4.106 One 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 the privacy principles.[131] The issue of due diligence in the context of mergers and acquisitions has also been raised in this Inquiry.[132]

4.107 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. The OPC has published an information sheet in relation to the obligations of buyers and sellers under the *Privacy Act*.[133] The OPC reported that it has not received a complaint about a breach of privacy during a due diligence exercise. The OPC stated that it is not practical to require an organisation in

---

127 See *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(c).
128 See *Privacy Act* RS 1985, c P-21 (Canada) s 8(j).
129 H Ruglen, *Submission PR 39,* 27 June 2006; Link Market Service, *Submission PR 2,* 24 February 2006.
130 Link Market Service, *Submission PR 2,* 24 February 2006.
131 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].
132 G Hill, *Consultation PC 21*, Melbourne, 8 May 2006.
133 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). This is available on the OPC's website.

the process of due diligence to gain the consent of everyone whose personal information is transferred.[134] The OPC recommended that the Australian Government should consider amending the NPPs to take into account the practice of due diligence.[135] The ALRC is interested in views as to whether such amendment is necessary, and if so, what form it might take. It is also interested in views about whether there is a need to amend Information Sheet 16 in this regard.

Alternative dispute resolution schemes

4.108 The OPC recommended that consideration be given to amending NPP 2 to enable use and disclosure of personal information during alternative dispute resolutions (ADR) used in the course of hearing disputes.[136] ADR involves a process, other than judicial determination, in which an impartial person helps those involved in a dispute to resolve their issues. Some submissions to the OPC Review stated that organisations have refused to disclose information needed by ADR schemes to investigate claims because of a concern that disclosure would breach the NPPs.[137] The ALRC is interested in hearing about experiences relating to the application of the privacy principles in the context of ADR schemes. Specifically, the ALRC is interested in views about whether legislative amendment to the privacy principles is needed and, if so, the content of such amendment.

Question 4–6 Is it desirable for the IPPs to deal separately with the principles relating to the use and disclosure of personal information or should use and disclosure be provided for in one principle?

Question 4–7 Are the circumstances in which agencies and organisations are permitted to use and disclose personal information under IPPs 10 and 11, and NPP 2, adequate and appropriate? In particular, should agencies and organisations be permitted expressly to disclose personal information: (a) to assist in the investigation of missing persons; (b) 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; and (c) in times of emergency? What mechanism should be adopted to establish the existence of an emergency?

---

134 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 191.

135 Ibid, Rec 57. See also *Privacy Act 1993* (NZ) s 6, Principle 11, which allows disclosure of information where 'it is necessary to facilitate the sale or other disposition of a business as a going concern'.

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 67. The OPC also recommended that NPP 10 be amended to allow for collection of sensitive information where necessary for the investigation and resolution of claims under an alternative resolution scheme. 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 67.

137 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 232.

Question 4–8 Are the criteria in NPP 2.1(a) for using personal sensitive and non-sensitive information for a secondary purpose adequate and appropriate? For example, is it necessary or desirable that there also be a 'direct' relationship between the secondary and primary purpose of collection before non-sensitive personal information can be used or disclosed for a secondary purpose?

Question 4–9 Is the scope of IPP 10(e) (which allows agencies to use personal information for a purpose other than the particular purpose of collection, if the purpose for which the information is used is directly related to the purpose of collection) adequate and appropriate? For example, should there be an additional requirement that the individual concerned would reasonably expect an agency to use the information for that other purpose?

Question 4–10 In what circumstances should agencies or organisations be required to record their use or disclosure of personal information when it is used or disclosed for a purpose other than the primary purpose?

Question 4–11 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?

Question 4–12 Is it appropriate that NPP 2 allows for personal non-sensitive information to be used for the secondary purpose of direct marketing? If so, are the criteria that an organisation needs to satisfy in order to use personal information for direct marketing purposes adequate and appropriate?

Question 4–13 Should use and disclosure of personal information be allowed for research that does not involve health information—for example social science research? If so, in what circumstances or upon what conditions might this be appropriate?

Principle 3: Data quality

4.109 NPP 3 provides that an organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

Gap in IPPs

4.110 Unlike NPP 3 and the OECD Guidelines, the IPPs do not contain a 'stand-alone' data quality principle. Aspects of the data-quality principle can be found in both IPP 3—which operates in relation to *collection* of information that is *solicited* by the collector—and IPP 8—which operates before a collector proposes to use the information. There appears to be a gap in the IPPs relating to the application of the data quality principle at the time of disclosure. In contrast, US privacy legislation imposes an obligation on agencies to ensure that, before disseminating any 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'.[138]

Issues relating to NPP 3

4.111 An issue arises as to whether it is desirable to extend the reach of NPP 3 to apply expressly to personal information that an organisation controls—which may not 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.[139]

4.112 An issue also arises whether NPP 3 should contain as part of the data quality principle the requirement that the information be relevant. Unlike the OECD Guidelines[140]—and, for example, Tasmanian privacy legislation[141]—NPP 3 does not include the requirement that the information be relevant as an aspect of the data quality principle. Rather, NPP 1 requires that at the stage of *collection* the information is necessary for one or more of the organisation's functions or activities. Unlike the NPPs, the IPPs contain an express requirement that information be relevant at the time of collection,[142] as well as a stand-alone principle requiring that personal information is to be used only for relevant purposes.[143]

4.113 One issue raised in the OPC Review concerned the interpretation of NPP 3. Some organisations consider that their obligations under NPP 3 to keep information up-to-date and accurate are absolute, and could be used to justify intruding upon an

---

138 *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 11 September 2006, Principle 10.

139 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, or a credit provider or credit reporting agency in 'possession or control' of a credit report.

140 See Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8.

141 *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 3.

142 *Privacy Act 1988* (Cth), s 14, IPP 3(c).

143 Ibid, s 14, IPP 9.

individual's privacy.[144] The OPC expressed the view that it is not reasonable to take steps to ensure data accuracy where this does not have any 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.[145] The ALRC is interested in hearing whether guidance by the OPC is an appropriate and effective response to this issue. As discussed below, Canadian privacy legislation makes it clear on its face that the obligation to maintain data quality is qualified.[146] Similarly, the Data Quality Principle in the OECD Guidelines qualifies the requirement that personal data be accurate, complete and up-to-date—the requirement only arises to the extent necessary for the purposes for which the data are to be used.

Question 4–14 Is the scope of the data quality principle in NPP 3 (which requires 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) adequate and appropriate? For example, should the principle expressly apply to information that an organisation controls?

Question 4–15 Is there a need to amend NPP 3 to clarify the extent of the obligations of an organisation under the data quality principle or is this best dealt with by way of guidance issued by the Office of the Privacy Commissioner?

Question 4–16 Should agencies be subject to a stand-alone data quality principle that extends to the collection, use and disclosure of personal information?

Principle 4: Data security

4.114 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.[147]

144 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.

145 See Ibid, Rec 79.

146 See *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) sch, Principle 4.6, and discussion below on Canadian principles.

147 Ch 8 discusses the difference between de-identified and identified information.

4.115 The OPC has issued an Information Sheet that explains an organisation's obligations in relation to physical security, computer and network security, communications security and personnel security.[148]

Gap in IPPs

4.116 NPP 4 picks up the Security Safeguards Principle in the OECD Guidelines. The main difference between NPP 4 and the Security Safeguards Principle and IPP 4 is that only NPP 4 imposes an obligation on an organisation to destroy or permanently de-identify personal information if it is no longer needed. One stakeholder queried why there was a principle in the *Privacy Act* limiting retention of data for the private but not the public sector.[149] This raises the issue of whether agencies should be under an obligation to destroy or permanently de-identify personal information when it is no longer needed. There is precedent for this position in the privacy legislation of Victoria, Tasmania and the Northern Territory.[150] The privacy legislation of New South Wales contains a requirement that an agency does not keep personal information for any longer than is reasonably necessary for the purposes for which the information may be lawfully used and that the information is disposed of securely and in accordance with the requirements for the retention and disposal of personal information.[151]

4.117 The US Federal Trade Commission concluded that a core data protection principle was integrity and security, which entailed collectors 'destroying untimely data or converting it to anonymous form'.[152] Canadian privacy legislation imposes an obligation on government institutions to dispose of personal information in their control in accordance with the regulations and any directives or guidelines issued by the designated Minister.[153] German privacy legislation also imposes an obligation on public bodies to erase personal data in certain circumstances.[154]

Disclosure of information to contractors

4.118 IPP 4, unlike NPP 4, imposes an express obligation on a record-keeper to take reasonable steps to prevent unauthorised use or disclosure of information contained in

148 See Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001).
149 G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.
150 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, IPP 4.2.
151 *Privacy and Personal Information Protection Act 1998* (NSW) s 12.
152 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998). This report is discussed further below.
153 *Privacy Act* RS 1985, c P-21 (Canada) s 6(3).
154 *Federal Data Protection Act 1990* (Germany) s 20(2).

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'.[155]

4.119 Given that NPP 4 does not specifically deal with the consequences of an organisation—including a non-government organisation and an unincorporated association—giving personal information to a contractor, the issue arises whether it should. One advantage of making specific provision in this area, and bringing it in line with IPP 4, is that it overcomes some of the problems that may arise where an organisation subcontracts to a small business that is not covered by the Act. The OPC recommended that the Australian Government should consider amending NPP 4 to impose an obligation on an organisation to ensure personal information it discloses to a contractor is protected.[156] The ALRC is interested in views as to whether the recommendation made by the OPC is effective to address the issue. German privacy law, for example, imposes obligations on both public and private bodies that commission agents to collect, process or use personal data. In each case, responsibility for compliance with data protection provisions rests with the principal.[157]

Deletion of personal information

4.120 Unlike NPP 4 and IPP 4, Victorian health privacy legislation as part of its 'data security and data retention' principle limits the circumstances in which a health service provider can delete information,[158] and sets out certain procedures to be followed where deletion is allowed.[159] 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—

---

155 *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.

156 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—OPC to issue guidelines to clarify that businesses that give personal information to contractors should impose contractual obligations on the contractor to take reasonable steps to protect the information.

157 See *Federal Data Protection Act 1990* (Germany) s 11.

158 *Health Records Act 2001* (Vic) sch 1, Health Privacy Principle (HPP) 4.2.

159 See Ibid sch 1, HPP 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. Health information privacy principles are discussed in Ch 8.

> whichever is the later.[160]

4.121 The issue arises whether the IPPs and NPPs should regulate the deletion of personal information—or any particular types of sensitive information—by organisations and agencies, or whether this is best left to guidelines. Regulation could involve legislative prohibition or authorisation of deletion in certain circumstances. An example of a legislative requirement to delete information arises in relation to certain information held on an individual's credit information file by a credit reporting agency.[161] German privacy law also imposes an obligation on 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.[162] The obligation is not dependent on a request being made by the individual concerned.

4.122 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.[163]

4.123 A related issue in this context is whether an individual should have the right to request an agency or organisation to destroy personal information—or sensitive information—that relates to him or her and, if so, in what circumstances or upon what conditions. Any such request would have to be considered having regard to obligations imposed by law to retain personal information for a period of time.

Question 4–17 Is the scope of NPP 4 relating to the obligations of an organisation to secure data adequate and appropriate? For example, should NPP 4 be amended to impose an obligation on organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected?

---

160 Ibid sch 1, HPP 4.2.

161 See *Privacy Act 1988* (Cth) s 18F.

162 *Federal Data Protection Act 1990* (Germany) s 35(2).

163 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).

Question 4–18 Are there any circumstances in which agencies should be under an obligation to destroy or permanently de-identify personal information when it is no longer needed?

Question 4–19 Should the IPPs and the NPPs regulate the deletion of personal information by organisations and agencies? In what circumstances might this be appropriate? Should an individual have the right to request that an agency or organisation destroy personal information that it holds or controls concerning the individual? If so, in what circumstances or upon what conditions should this be permitted?

Principle 5: Openness

4.124 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.[164] When requested by a person, an organisation must take reasonable steps to let the person know, generally, what sort of personal information it holds, for what purposes, and how it collects, holds, uses and discloses that information.[165]

Comparison with IPPs

4.125 Unlike NPP 5, the obligation imposed on a record-keeper under IPP 5 to take reasonable steps to enable a person to ascertain specified matters is not limited to where the person has made a request. Further, while NPP 5 imposes a general obligation on an organisation to maintain a document setting out its policies on the management of personal information, IPP 5 takes a more prescriptive approach. IPP 5 imposes an obligation to maintain a record that includes a number of detailed specified matters in relation to the agency's record-keeping practice, as well as an annual obligation to provide the Privacy Commissioner with a copy of the record.

Issues relating to NPP 5

4.126 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'.[166] The issue arises whether NPP 5 should be amended to clarify the openness principle. The OPC

164 *Privacy Act 1988* (Cth) sch 3, NPP 5.1.
165 Ibid sch 3, NPP 5.2.
166 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 91.

recommended that the Australian Government should consider amending NPP 5.1 to provide for short form privacy notices, which 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.[167] It suggested that short form notices 'would improve the quality of an organisation's communication with its customers'.[168]

4.127 The OPC said:

> A long privacy notice may not fulfil its purpose of informing a consumer because the consumer may be overwhelmed and confused because it is too long. 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.
>
> 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.[169]

4.128 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.[170] The ALRC is interested in views on the use of short form privacy notices.

Question 4–20 Is the scope of NPP 5 relating to openness adequate and appropriate? For example, is it necessary or desirable for organisations to be given greater legislative guidance about their obligations under the principle? Does the more prescriptive approach to the openness principle in IPP 5 provide a suitable model?

Question 4–21 Is it appropriate that certain obligations under the NPPs relating to openness are triggered only upon an individual's request?

167 Ibid, Rec 19.
168 Ibid, 91.
169 Ibid, 92.
170 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).

Question 4–22 Is there a need to clarify the relationship between the obligation of an organisation under NPP 1.3 (which imposes an obligation on organisations to take reasonable steps to ensure that an individual is aware of specified matters at or before the time of collection) and NPP 5.1 (which imposes an obligation on organisations to set out in a document clearly expressed policies on its management of personal information)? If so, how is this best achieved?

Principle 6: Access and correction

4.129 NPP 6.1 sets out the general principle that if an organisation holds personal information about an individual, it must allow the individual to access the information on request. However, access does not have to be given if:

- 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;
- in the case of health information, providing access would pose a threat to the life or health of any individual;
- providing access would have an unreasonable impact upon the privacy of other individuals;
- the request for access is frivolous or vexatious;
- 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;
- 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;[171]
- providing access would be unlawful;[172]
- denying access is required or authorised by law;

171 For example, where an organisation is currently negotiating with an individual about the purchase of an object and is seeking independent valuation: See Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [374(f)].

172 For example, if providing access would ground an action for breach of confidence: Ibid, [374(g)].

- providing access would be likely to prejudice an investigation of possible unlawful activity;

- providing access would be likely to prejudice by or on behalf of an enforcement body: the prevention, detection, investigation, prosecution or punishment of criminal offences, or breaches of a law imposing a penalty or sanction; the enforcement of laws relating to the confiscation of proceeds of crime; the protection of the public revenue; the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or the preparation for, or conduct of, proceedings before any court or tribunal or the implementation of its orders; or

- 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.

4.130 NPP 6.2 allows an organisation to give an individual an explanation for a commercially sensitive decision rather than providing direct access to information, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process.

4.131 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.[173]

> The sub-principle 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.[174]

4.132 NPP 6.4 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.

4.133 NPP 6.5 provides that if an individual is able to establish that personal information about the individual held by an organisation 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

---

173 *Privacy Act 1988* (Cth) sch 3, NPP 6.3. Compare *Privacy Act 1988* (Cth) s 18H, which allows, in certain circumstances, an individual's rights of access to credit information files and credit reports to be exercised by another person authorised in writing by the individual.

174 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).

individual asks the organisation to associate with the information a statement claiming the information is not accurate, complete or up-to-date, the organisation must take reasonable steps to comply with the request.[175]

4.134 Finally, NPP 6.7 provides that an organisation must provide reasons for denial of access or a refusal to correct personal information.

4.135 Some exceptions to access—such as those relating to law enforcement functions and the investigation of unlawful activity—are the same or similar to exceptions to disclosure in NPP 2. However, some exceptions to access differ from the exceptions to disclosure without any apparent policy justification. For example, it is not clear why an organisation is permitted to disclose information to a third party where it reasonably believes that the use or disclosure is necessary to lessen or prevent a serious and imminent threat to an individual's safety but is not authorised to withhold access by an individual to his or her personal information where providing access would pose a similar threat to an individual's safety. For example, in other contexts, the law recognises that in certain circumstances it may be harmful to allow a person access to specified information contained in his or her medical records.[176] In this regard, the privacy legislation of New Zealand allows an agency to refuse an individual access to his or her personal information where such access would be likely to endanger the safety of any individual.[177]

Comparison with OECD Guidelines, IPPs and other legislation

4.136 NPP 6 is consistent with parts of the Individual Participation Principle and the Data Quality Principle in the OECD Guidelines[178] but there are some key differences. While both the Individual Participation Principle and NPP 6 provide that access to data or information should not be provided at an excessive cost,[179] only the Individual Participation Principle makes provision concerning the time in which data are to be communicated, and the manner and form of that communication. NPP 6, for example, does not provide that access to personal information should be provided within a reasonable time and in a reasonable manner.[180] In contrast, Victorian privacy legislation sets out the timeframe within which a request for access to, or correction of,

175 *Privacy Act 1988* (Cth) sch 3, NPP 6.6.
176 See *Mental Health Act 1990* (NSW) s 45.
177 *Privacy Act 1993* (NZ) s 27(1)(d).
178 However, as discussed above, NPP 3 is the main principle dealing with data quality.
179 Compare *Federal Data Protection Act 1990* (Germany) ss 19 and 34(5), which provide that information is to be provided by public and private bodies to the data subject free of charge, subject to some exceptions for private bodies.
180 The timeframe for access is addressed in Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 49.

personal information must be acted upon.[181] Further, unlike the Individual Participation Principle, NPP 6 does not confer on an individual an express right to challenge a denial of access.

4.137 There are also differences between NPP 6 and IPPs 6 and 7—which deal separately with access and correction. A key differences is that NPP 7, unlike IPP 6, specifies many exceptions to the access principle. IPP 6 generally provides that an individual has a right of access except to the extent that the record-keeper is entitled or authorised to refuse access under provisions of any Commonwealth law that provide for access by persons to documents.[182] This raises the issue of whether IPP 6 should set out more clearly the circumstances in which agencies can deny an individual access to his or her personal information. Unlike IPP 6, NPP 6 provides for the possibility of a compromise where access to information is denied under one of the specified exceptions: the organisation is to consider the use of mutually agreed intermediaries. Also, unlike IPP 6, NPP 6 expressly requires an organisation to give reasons for denial of access.

4.138 One difference between NPP 6 and IPP 7 is that NPP 6 expressly imposes as a prerequisite to correction that an individual establish that information is not accurate, complete and up-to-date. Another difference is that, in the event that there is a disagreement about correction, IPP 7 requires the record-keeper to 'attach' to the record, on request, any statement provided by the individual of the correction sought. NPP 6 requires the organisation, on request, to 'associate' with the information a statement that it is not accurate, complete or up-to-date.

> 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.[183]

4.139 Unlike access to government records, there are no formal mechanisms in place to facilitate access to personal information held by organisations. Although the OPC provides guidance and information sheets on the topic,[184] it is up to each organisation to develop access procedures.

4.140 A minor issue that arises when one compares NPP 6 to comparable state and territory provisions is that other provisions, insofar as they relate to the exception dealing with existing or anticipated legal proceedings, cover information that would

---

181 See *Information Privacy Act 2000* (Vic) sch 1, IPP 6.8 (request to be actioned no later than 45 days after receipt).

182 As noted above, the two main pieces of legislation regulating access to documents are the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth).

183 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–4810]. See also *Privacy Act 1988* (Cth) s 18J which imposes an obligation on 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.

184 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).

not be accessible by the processes of discovery or subpoena.[185] The exception in NPP 6 is limited to discovery. The question arises whether it is necessary or desirable to amend NPP 6 to include a reference to information not accessible by subpoena where that information relates to existing or anticipated legal proceedings between the organisation and the individual.

Issues relating to NPP 6

4.141 Submissions to the OPC Review identified a number of issues and concerns in relation to NPP 6. These include: concerns that in the health care context, particularly in the mental health care context, allowing an individual to access his or her medical records could harm the patient or interfere with the therapeutic relationship;[186] that the obligation for an organisation merely to 'consider' the use of an intermediary where it is not required to provide access, was inadequate;[187] that, because there is no maximum fee or schedule of fees in the *Privacy Act* for accessing personal information, organisations are charging a wide variety of fees;[188] that it was too onerous to require an individual to 'establish' the inaccuracy of personal information as a prerequisite to correction by the organisation;[189] and that there is a gap in the legislation as it does not require an organisation, having responded to a request to correct inaccurate personal information, to notify any third parties that received inaccurate personal information.[190] The OPC made a number of recommendations to address these concerns, one of which involves legislative amendment:

> 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.[191]

4.142 However, the OPC's recommendation does not go so far as to require an organisation to pass on corrected information to third parties who have received inaccurate information. The EU Directive, for example, requires Member States to guarantee that every data subject has the right to obtain from the controller

185 See, eg, *Information Privacy Act 2000* (Vic) sch 1, IPP 6.1(d) (applicable to the public sector); *Information Act 2002* (NT) sch, IPP 6.1(e) (applicable to the public sector).
186 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 113, 115.
187 Ibid, 114, 116.
188 Ibid, 114, 116.
189 Ibid, 116.
190 Ibid, 116, 117.
191 Ibid, Rec 28.

> notification to 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.[192]

4.143 Similarly, the US 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'.[193]

4.144 NPP 6 does not impose an obligation on an organisation to alert third parties where it has refused to make a correction pursuant to an individual's request. The ALRC is interested in views on whether such a requirement should be imposed on organisations and agencies. For example, Canadian privacy legislation imposes a requirement on organisations, where appropriate, to transmit to third parties corrected personal information, or to alert those parties to the existence of an unresolved challenge concerning the accuracy of the personal information.[194] Canadian privacy legislation also requires a government institution, in certain circumstances, to notify third parties to whom it has disclosed information of a correction made to that information, or of a notation where the correction is not made. Where the disclosure is to a government institution, the institution is to make the correction or notation on any copy of the information under its control.[195] German privacy law also requires public and private bodies to 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'.[196]

4.145 Many of the recommendations in the OPC Review do not involve amendment of NPP 6 but focus on the provision of further guidance by the OPC. Guidance is recommended in relation to the interpretation of NPP 6—specifically that a serious threat to a therapeutic relationship could be a serious threat to a person's health;[197] and the meaning of the requirement that an individual 'establish' that information is not accurate[198]—as well as in relation to fees to access personal information.[199]

---

192 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).

193 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998), 9. This report is discussed further below.

194 *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) sch 1, Principles 4.9.5, 4.9.6.

195 *Privacy Act* RS 1985, c P-21 (Canada) s 12(2).

196 *Federal Data Protection Act 1990* (Germany) ss 20(8), 35(7).

197 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 30. This issue is discussed further in Ch 8.

198 Ibid, Rec 32. Compare *Federal Data Protection Act 1990* (Germany) s 35(2) which contains a reverse onus of proof insofar as it requires a private sector body to erase certain categories of personal data where it cannot prove that they are correct.

199 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

4.146 Are some of the areas in respect of which the OPC has recommended further guidance more appropriately dealt with by legislative amendment, either to the primary legislation or by way of regulation? Some advantages of legislative amendment are that it promotes clarity and certainty of approach. Guidelines are generally not legally binding but promote a more flexible and 'light touch' approach to compliance. The ALRC is interested in views on this issue.

IPP issues

4.147 Some of the issues relating to access and correction identified above also apply to the IPPs. For example, the IPPs do not impose a requirement on an agency to notify third parties of any amendments it has made to an individual's personal information, or of the fact that it has refused to make a correction sought by the individual affected. In contrast, the privacy legislation of New South Wales, for example, 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.[200]

Question 4–23 Are the circumstances in which organisations can deny an individual access to his or her personal information under NPP 6 adequate and appropriate? If the circumstances are inadequate, should this be addressed by legislative amendment to the principle or by guidance issued by the Office of the Privacy Commissioner?

Question 4–24 Should IPP 6 more clearly set out the circumstances in which agencies can deny an individual access to his or her personal information? If so, what circumstances should be included?

Question 4–25 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?

Principle 7: Identifiers

4.148 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

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 Ch 8.

200 *Privacy and Personal Information Protection Act 1998* (NSW) s 15(3).

organisation's operations' and excludes an individual's name or ABN from the definition. An example of an Australian Government identifier is a Medicare number.

4.149 NPP 7.1 provides that an organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by an agency. An organisation is also prohibited from adopting as its own identifier, an identifier of an individual that has been assigned by an agent of an agency or a contracted service provider for a Commonwealth contract.[201]

> For example, it 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.[202]

4.150 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, namely those involving threats to an individual's life, health, or safety; public health or public safety; investigation or reporting of suspected unlawful activity; specified functions by or on behalf of an enforcement body; or where the use or disclosure is required or authorised by law;[203] or
- is by a prescribed organisation of a prescribed identifier in prescribed circumstances.[204]

4.151 The 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.[205]

4.152 Chapter 12 discusses the history of identification schemes in Australia, and issues and concerns relating to the use of multi-purpose identifiers—in particular, the practice of data-matching.

---

201 *Privacy Act 1988* (Cth) sch 3, NPP 7.1A, however, allows for the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances. See *Privacy (Private Sector) Regulations 2001* (Cth) reg 7. See also *Privacy Act 1988* (Cth) s 100(2).

202 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [380].

203 See *Privacy Act 1988* (Cth) sch 3, NPP 2.1(e)–(h).

204 A number of regulations have been passed in this regard. See *Privacy (Private Sector) Regulations 2001* (Cth) regs 8, 9, 10, 11.

205 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 269.

4.153 The OECD Guidelines and the IPPs do not contain any principle equivalent to NPP 7.

Issues relating to NPP 7

Is there a need for a separate principle to regulate identifiers?

4.154 A preliminary issue that arises is whether there is a need for a separate principle regulating 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, that part of NPP 7 that bans the adoption by an organisation of an identifier assigned by an agency could be accommodated within the privacy principles governing use of personal information. But, as discussed below, some submissions have identified particular issues relating to the collection, use and disclosure of identifiers. The ALRC is interested in views on this issue, and, in particular, whether the principle regulating identifiers should be redrafted to deal more generally with the issue of data-matching.

Collection of identifiers

4.155 Issues relating to IPP 7 were raised in the OPC Review. Submissions expressed concern in relation to 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.[206] NPP 7 does not prohibit the collection of identifiers. The OPC expressed the view that there did 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:

> if 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.[207]

4.156 The ALRC is interested in views about whether the collection of unique identifiers should be addressed separately and specifically in the NPPs.

Exceptions to the use and disclosure of identifiers

4.157 Some submissions to the OPC Review suggested that it would be beneficial to allow another exception to the limitation upon the use and disclosure of Australian Government identifiers. This exception would allow individuals to consent to the use

206 Ibid, 270.
207 Ibid, 272.

or disclosure of their identifiers.[208] This arguably would allow organisations to provide concessional services more efficiently. For example, an organisation may want to check with an Australian Government agency to confirm that an individual is a customer of that agency and therefore entitled to a concession rate from the organisation. The organisation could collect an individual's Centrelink customer reference number and pass it onto Centrelink to confirm the individual's eligibility for concessions. This practice, however, may be prohibited under NPP 7.[209] 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.[210]

4.158 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 risk of the widespread collection, use and disclosure of Australian Government identifiers.[211] 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.[212] 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 in this regard.[213] The ALRC is interested in views about whether individuals should be able to consent to the use of their identifiers, and if so, in what circumstances and by what means should such exception be given effect.

Definition of identifier

4.159 Another issue is whether the definition of identifier can be improved. The definition in NPP 7 does not describe what an identifier is, only what it includes. 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

---

208 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. See Confidential, *Submission PR 32,* 2 June 2006.

209 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 270.

210 Ibid, 271.

211 Ibid, 272.

212 Ibid, Rec 80. In this regard see *Privacy (Private Sector) Regulations 2001* (Cth) reg 9.

213 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).

identifier that consists only of the individual's name'.[214] 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. [215]

Gap in IPPs

4.160 The IPPs do not contain a provision comparable to NPP 7. Some state and territory legislation regulates the assignment, adoption, use and disclosure of identifiers by public sector bodies. This is generally prohibited unless it is necessary for the body to carry out its functions efficiently.[216] Insofar as those state and territory provisions regulate the assignment of identifiers, they go further than NPP 7. NPP 7 is silent on the assignment of identifiers by organisations. It prohibits the adoption by organisations of Commonwealth identifiers that have already been assigned. There is a gap in the IPPs insofar as they do not regulate the assignment, adoption, use and disclosure of identifiers. The ALRC is interested in hearing whether it is necessary or desirable that this gap be filled.[217]

Question 4–26 Is there a need for a separate privacy principle regulating the adoption, collection, use and disclosure of identifiers by organisations? Should NPP 7, the principle regulating identifiers, be redrafted to deal more generally with the issue of data-matching?

Question 4–27 Is the definition of identifier adequate and appropriate? Are the exceptions to the use and disclosure of identifiers referred to in NPP 7 adequate and appropriate? Should an individual be permitted to consent to the use of his or her unique identifier? If so, in what circumstances and by what means should this exception be given effect?

Question 4–28 Should the *Privacy Act* be amended to regulate the assignment, adoption, collection, use and disclosure of identifiers by agencies?

---

214 See *Information Privacy Act 2000* (Vic) sch 1.
215 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 55.
216 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).
217 For a discussion of data-matching and tax file numbers—a type of identifier—see Ch 7.

Principle 8: Anonymity

4.161 NPP 8 provides that, wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

4.162 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 states:

> 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.[218]

4.163 NPP 8 complements NPP 1 which prohibits an organisation from collecting information that is not necessary for its functions or activities. NPP 8 is intended to affect the design of new technologies that collect more information than is necessary when transacting with individuals.[219]

4.164 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.[220]

4.165 Where an individual wishes to open a bank account or where reporting requirements are imposed in relation to notifiable diseases are examples of where the law may require an organisation to identify an individual with which it is dealing.[221]

4.166 The OECD Guidelines and the IPPs do not contain a comparable anonymity principle; neither do the privacy statutes of New Zealand or the United Kingdom (UK).[222] The issue arises whether there should be an anonymity principle imposed on Commonwealth agencies. Professor Graham Greenleaf is of the view that the IPPs should contain an anonymity principle.[223] As noted below, German privacy law

---

218 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [384].
219 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5510].
220 Ibid, [2–5520].
221 Ibid, [2–5530].
222 See *Privacy Act 1993* (NZ) s 6; *Data Protection Act 1998* (UK) sch 1.
223 G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

imposes obligations in relation to anonymity on both public and private sector bodies.[224] Victorian and Tasmanian privacy legislation contain an anonymity principle along the lines of NPP 8, which applies to public sector bodies.[225] The Northern Territory legislation also contains an anonymity principle applicable to public sector organisations but it is drafted in different terms to NPP 8, insofar as it expressly identifies the obligation imposed on an organisation.

> 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.[226]

4.167 An issue arises as to whether NPP 8 may be better drafted by imposing expressly an obligation on an organisation to give an individual the option of remaining anonymous when entering into transactions with that organisation.

Question 4–29 Should NPP 8, the anonymity principle, be redrafted to impose expressly an obligation on organisations to give an individual the option of remaining anonymous when entering into transactions with those organisations?

Question 4–30 Is it appropriate or desirable for agencies to be subject to an anonymity principle? In what circumstances, if any, might this be appropriate?

Principle 9: Transborder data flows

4.168 NPP 9 specifies the circumstances in which an organisation in Australia or an external territory can transfer information about an individual to someone—other than the organisation or the individual—who is in a foreign country.[227] Those circumstances are:

- if the organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract that effectively upholds principles for fair handling of the information that are substantially similar to the NPPs;
- the individual consents to the transfer;

224 See *Federal Data Protection Act 1990* (Germany) s 3a.
225 *Information Privacy Act 2000* (Vic) sch 1, IPP 8.1; *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 8.
226 *Information Act 2002* (NT) sch, IPP 8.
227 Transborder data protection is discussed in Ch 13.

- 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;

- 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;

- the transfer is for the individual's benefit; it is impracticable to obtain the individual's consent; and if it were practicable to obtain such consent the individual would be likely to give it; or

- the organisation has taken reasonable steps to ensure that the information that it has transferred will not be held, used, or disclosed by the recipient of the information inconsistently with the NPPs.[228]

4.169 While NPP 9 does not apply to transfers of personal information outside Australia by an organisation to another part of the same organisation, a company transferring personal information overseas to a related company must comply with NPP 9.[229]

4.170 NPP 9 is based on the restrictions on international transfers of personal information set out in the EU Directive dealing with the processing of personal data.[230]

4.171 Examples of organisations transferring personal information overseas include: a travel agency disclosing a traveller's itinerary details to an overseas hotel; an importer disclosing the stock requirements of an individual's business to its supplier; and a stockbroker disclosing details about a client's investment account to an agent operating in a foreign stock exchange.[231]

4.172 Chapter 13 raises the issue of whether NPP 9 provides adequate and appropriate protection for personal information transferred outside Australia. It also discusses criticisms of NPP 9, including the lack of guidance regarding countries whose regimes provide adequate protection equivalent to the NPPs.

4.173 The IPPs and OECD Guidelines do not contain a comparable transborder data principle. The difference between the IPPs and the NPPs in this regard was noted in a consultation.[232] Should the transfer of personal information offshore by agencies also

---

228 *Privacy Act 1988* (Cth) sch 3, NPP 9(f).
229 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58.
230 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 25. Article 25(1) is set out in Ch 13.
231 See J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2–5760].
232 M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006.

be regulated? Some state and territory privacy legislation contains a transborder principle regulating the transfer, by public sector bodies, of data outside the particular state or territory.[233] German privacy law also imposes obligations concerning transborder flows on both public and private sector bodies.[234]

Question 4–31 Should the transfer of personal information offshore by agencies be regulated by privacy principles?

Principle 10: Sensitive information

4.174 NPP 10 prohibits the collection of sensitive information, except in certain identified circumstances. Sensitive information is defined in s 6 of the *Privacy Act*. The definition is discussed in Chapter 3.

4.175 NPP 10.1 provides that sensitive information can be collected only if:

- the individual has consented;
- the collection is required or authorised by or under law;[235]
- 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 consent to the collection, or physically cannot communicate consent to the collection; or
- the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

4.176 In addition, NPP 10.1 allows sensitive information to be collected in the course of the activities of a non-profit organisation.[236] 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.

---

233 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, IPP 9.

234 See *Federal Data Protection Act 1990* (Germany) s 4(b).

235 See *Privacy Legislation Amendment Act 2006* (Cth).

236 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.

4.177 NPP 10.2 provides that despite NPP 10.1 an organisation may collect health information[237] about an individual if:

- the information is necessary to provide a health service to the individual; and
- the information is collected as required by law (other than the *Privacy Act*), or in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality that bind the organisation.[238]

4.178 NPP 10.3 provides that, despite NPP 10.2, an organisation may collect health information about an individual if:

- the information is collected for any of the following purposes: 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;
- 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;
- 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 by the Privacy Commissioner under s 95A of the *Privacy Act*.

4.179 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.

Comparison with OECD Guidelines, IPPs and other legislation

4.180 The OECD Guidelines and the IPPs do not contain a comparable principle relating to the collection of sensitive information. Indeed, the Explanatory

237 Health information is a category of sensitive information. Issues concerning the collection of health information are discussed in Ch 8.

238 See also *Privacy Legislation Amendment Act 2006* (Cth) sch 1.

Memorandum to the OECD expresses the view that 'it is probably not possible to identify a set of data which are universally regarded as being sensitive'.[239]

4.181 The issue arises whether Commonwealth agencies should be subject to restrictions in relation to the collection of sensitive information. Under Victorian, Tasmanian and Northern Territory privacy legislation, agencies are subject to restrictions in relation to the collection of sensitive information.[240] However, the exceptions to the prohibition on collection of sensitive information by agencies in some state and territory privacy legislation are wider than those set out in NPP 10. For example, the legislation of Victoria and the Northern Territory allows a public sector body to 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;[241]
- 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.[242]

4.182 This raises the issue of whether agencies and organisations should be able to collect non-health related sensitive information for certain purposes, including research and statistical purposes, and in what circumstances this should be permitted. For example, German privacy legislation allows public and private bodies to collect 'special categories of personal data'[243]—a concept similar to 'sensitive information'—if

> it is necessary for scientific research purposes and the scientific interest in carrying out the research project substantially outweighs the data subject's interest in opposing collection and the purpose of the research could not be achieved by other means or without unreasonable effort or at all.[244]

4.183 The privacy legislation of the UK allows sensitive information concerning racial or ethnic origin to be collected if it is necessary for identifying and monitoring the

---

239 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [19(a)].

240 *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.

241 See also *Personal Information Protection Act 2004* (Tas) sch 1, PIPP 2(c).

242 *Information Privacy Act 2000* (Vic) sch 1, IPP 10.2; *Information Act 2002* (NT) sch, IPP 10.2.

243 See *Federal Data Protection Act 1990* (Germany) s 3.

244 See Ibid ss 13(2)(8), 28(6)(4).

existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to promoting or maintaining equality.[245]

Issues relating to NPP 10

4.184 The ALRC is interested in views as to whether the current exceptions to the prohibition on collection of sensitive information are adequate and appropriate. 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 in many situations 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'. Given that similar wording is used in one of the exceptions in NPP 10, the issue arises as to whether legislative amendment is necessary specifically to allow for the collection of sensitive information in emergency situations, including disaster recovery, where the individual is not in a position to give consent. In this regard, 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'.[246]

4.185 The Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 makes specific provision for the collection of personal information for permitted purposes in times of emergencies and disasters.

A separate regime for regulating sensitive information?

4.186 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 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'.[247] NPP 10 imposes restrictions on the collection of sensitive information, and, as discussed above, NPP 2 distinguishes between sensitive and non-sensitive information in the context of particular obligations of an organisation concerning use and disclosure. However, the NPPs do not cover the field in relation to the regulation of sensitive information in all aspects of the information cycle. Should federal privacy

245 *Data Protection Act 1998* (UK) sch 3, cl 9.
246 *Federal Data Protection Act 1990* (Germany) s 13.
247 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.

principles establish a separate and complete regime for the public and private sectors regulating sensitive information in all aspects of the information cycle, including collection, use, disclosure, access, retention and disposal? The ALRC is interested in views on this issue.

4.187 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 information,[248] while others, such as the UK[249] and Germany,[250] do to varying extents. The privacy legislation of New South Wales makes a distinction between the disclosure of sensitive and non-sensitive information.[251]

Question 4–32 Should federal privacy principles allow agencies and organisations to collect non-health related sensitive information for other purposes, including research and statistical purposes? If so, in what circumstances should this be permitted?

Question 4–33 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?

One set of principles?

4.188 A recurring issue in the inquiries undertaken by the OPC, the Senate Legal and Constitutional References Committee, the Taskforce on Reducing Regulatory Burdens on Business, and the ALRC's current Inquiry, is whether maintaining two separate sets of sometimes inconsistent principles for the public and private sectors can continue to be justified.[252] The question arises whether it would be desirable and cost-effective from a compliance perspective to have a single set of privacy principles regulating both sectors or whether some principles need to be adapted to meet the exigencies of either sector. For example, special principles may need to apply to the public sector because it can compel the production of personal information, and the private sector may need a specific principle dealing with direct marketing.[253]

248 *Privacy Act 1993* (NZ).
249 *Data Protection Act 1998* (UK) sch 1, Principle 1; sch 3.
250 *Federal Data Protection Act 1990* (Germany).
251 *Privacy and Personal Information Protection Act 1998* (NSW) ss 18, 19.
252 Chs 2 and 7 discuss the broader issue of national consistency.
253 Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006.

4.189 As noted above, the OECD Guidelines apply to both the public and private sectors. The Asia-Pacific Economic Cooperation (APEC) principles also apply to both the public and private sectors.[254] There is precedent in other jurisdictions for having a single set of principles applying to both the public and private sectors,[255] as well as for having separate principles or provisions regulating the public and private sectors.[256]

4.190 There are circumstances when 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 and will also be bound by contract to comply with the IPPs.[257] Some government 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.[258]

4.191 The OPC stated that:

> 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.[259]

4.192 The OPC Review 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.[260]

4.193 Submissions to the Senate Committee privacy inquiry and to the Taskforce on Reducing Regulatory Burdens on Business expressed concern about the inconsistency

---

254 The APEC principles are discussed below. The Australian Government is currently working on a number of issues relating to the domestic and international implementation of the APEC Privacy Framework. See Privacy Professionals, *Consultation PM 11*, Sydney, 3 August 2006; Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

255 See *Privacy Act 1993* (NZ) s 2 (definition of agency) and s 6.

256 See, eg, *Privacy Act* RS 1985, c P-21 (Canada) (regulation of public sector); *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) (regulation of private sector). These Acts are discussed further below.

257 See *Privacy Act 1988* (Cth) ss 95B, 6A(2).

258 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.

259 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 46.

260 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.

within the *Privacy Act* resulting from two sets of principles.[261] Submissions also noted that two separate regimes caused particular difficulties in the health sector, where public and private health organisations often work closely together.[262] Some have expressed concern that the separation of the NPPs and IPPs creates complexity in public and private partnerships.[263] Other have submitted that the distinction between the public and private sectors is not helpful and should be avoided.[264] Support was expressed for the rationalisation and development of a single set of privacy principles.[265] Reasons given for this approach included the desirability of achieving national consistency and simplicity, as well as administrative convenience.[266] The number of similarities between the IPPs and NPPs appear to make the task of rationalisation feasible.

4.194 The issue also arises as to whether separate principles or subsets of principles should apply to particular areas of regulation, such as telecommunications,[267] or to particular types of personal information, such as health information[268] or credit information.[269]

Model of principles to be adopted?

4.195 If one set of principles were to be developed, the issue arises as to which model should be adopted. A number of stakeholders have expressed the view that the NPPs—though capable of improvement—are superior to the IPPs.[270] The privacy Acts of

---

261 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.

262 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.37].

263 For example, G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

264 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006.

265 For example, Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; D Lindsay, *Consultation PC 25*, Melbourne, 9 May 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006; Australian Government Department of Foreign Affairs and Trade, *Consultation PC 10*, Canberra, 29 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; Federal Privacy Commissioner, *Consultation PM 2*, Sydney, 23 February 2006.

266 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006.

267 The application of the privacy principles in the telecommunications area is discussed in Ch 10.

268 Health information principles are discussed in Ch 8.

269 The relationship between the credit reporting provisions of the *Privacy Act* and the privacy principles will be considered in a separate Issues Paper.

270 For example, D Antulov, *Submission PR 14,* 28 May 2006; M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006; M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 2006; Privacy

Victoria, Tasmania and the Northern Territory[271] are largely based on the NPPs—although they are not 'word for word' replicas. 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'.[272] In contrast, the privacy legislation of New South Wales is largely based on the IPPs[273] and the privacy schemes in Queensland and South Australia also adopt the IPPs.[274]

4.196 One stakeholder expressed the view 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.[275] 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. The more radical any departure from those principles, the greater the consequential compliance burden that will be imposed. The OPC concluded that the NPPs 'have worked well and delivered to individuals protection of personal and sensitive information in Australia in those areas covered by the Act'.[276] However, as noted above, the Senate Committee privacy inquiry disagreed with the OPC's conclusion that the private sector provisions are 'working well'.[277]

4.197 To inform the determination of which model of principles, or whether any specific principle, should be adopted it is convenient also to consider the models of information privacy principles that have been adopted in other jurisdictions. The discussion below addresses the models of the US, Canada, Germany and the UK.

Overseas jurisdictions

United States

4.198 Fair Information Practice Principles (FIPPs) were first set out in the US Department of Health, Education and Welfare's Report, *Records Computers and the*

Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006; G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

271 See *Information Privacy Act 2000* (Vic) sch 1; *Personal Information Protection Act 2004* (Tas) sch 1; *Information Act 2002* (NT) sch. See also Ch 2.

272 See *Personal Information Protection Act 2004* (Tas) s 3.

273 See *Privacy and Personal Information Protection Act 1998* (NSW) pt 2, div 1.

274 See Queensland Government Department of Justice and Attorney-General, *Privacy* (2005) <www.justice.qld.gov.au/dept/privacy.htm> at 26 June 2006; South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992). See also Ch 2.

275 R Clarke, *Consultation PC 14*, Canberra, 30 March 2006.

276 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.

277 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.27].

Rights of the Citizen.[278] That report called on Congress to adopt a Federal Code of Fair Information Practice based on five basic principles, namely:

> 1. There must be no personal data record-keeping systems whose very existence is secret.
>
> 2. There must be a way for a person to find out what information about the person is in a record and how it is used.
>
> 3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
>
> 4. There must be a way for an individual to correct or amend a record of identifiable information about him.
>
> 5. Any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[279]

4.199 These principles can be described in more contemporary terms as transparency, use limitation, access and correction, data quality and security.[280] They formed the basis for the *Privacy Act*, adopted by Congress in 1974.[281] That Act governs the collection and use of personal information by the public sector. The Act, for example, precludes disclosure by an agency of a record relating to an individual except pursuant to a written request from, or with the prior written consent of, the individual to whom the record relates, except in defined circumstances.[282]

4.200 In 1998, the US Federal Trade Commission (FTC) having reviewed 'fair information practice codes' of the US, Canada and Europe, concluded that there were five core principles of data protection, namely:

> 1. **Notice/Awareness:**—The most fundamental principle is notice. … Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.
>
> 2. **Choice/ Consent:**—… At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information …
>
> 3. **Access/Participation:**—Access … refers to an individual's ability both to access data about him or herself … and to contest that data's accuracy and completeness.

---

278 United States Government Department of Health Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973).

279 Ibid.

280 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 2006) Ch 14, 4.

281 *Privacy Act 1974* 5 USC § 552a (US). See also United States Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).

282 See *Privacy Act 1974* 5 USC § 552a (US).

> 4. **Integrity/Security:—**Data must be accurate and secure. …
>
> 5. **Enforcement/Redress:**—… Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive and does not ensure compliance with fair information practice principles.[283]

4.201 In 2000, the FTC issued another privacy report to Congress, which removed enforcement/redress as a core principle, thereby reducing the list to four core principles.[284]

4.202 Unlike the OECD Guidelines, the APEC principles, the NPPs and the IPPs, the core principles identified by the FTC do not include a collection limitation principle: collectors are free to collect whatever data they wish so long as they provide accurate notice.[285]

4.203 In addition to federal privacy principles, there are state privacy principles in the US, which vary from state to state.[286] A particular requirement under Californian law in relation to the reporting of breaches is set out below.

California model on reporting breaches

4.204 The IPPs and NPPs do not impose an obligation on agencies and organisations to notify individuals whose personal information has been compromised. It has been reported that 22% of respondents to a survey of Australian public and private sector organisations have experienced 'electronic attacks that harmed the confidentiality, integrity or availability of network data or systems'.[287] In August 2005 a server in an Australian payment gateway provider was unlawfully accessed, exposing the details of 46,000 credit cards.[288]

4.205 The Californian model has a mandatory provision for the reporting of security breaches. Section 1798.29(a) of the *California Civil Code* provides:

> Any agency that owns or licences computerised data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person.
>
> The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as

283 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998).
284 United States Government Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress* (2000).
285 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 2006) Ch 14, 13.
286 Ibid, 26. The US Safe Harbor privacy principles are discussed in Ch 13.
287 N Miller, 'Data Leaks Under Review', *The Sydney Morning Herald* (Sydney), 8 August 2006, 27.
288 Ibid.

> provided for in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

4.206 The Californian notification law has been a model for legislation passed by other US state legislatures, and there are moves to implement a national notification standard concerning compromised data.[289] However, there are differences in the approaches that the states have taken, and a key issue is ascertaining what types of data breaches should trigger notices to consumers. Should it extend to any unauthorised disclosure or only those disclosures that could lead to harm, such as identity theft?[290]

4.207 Karen Curtis, the Privacy Commissioner, has expressed support for organisations to adopt the practice of notifying individuals when a breach of security leads to the disclosure of personal information.[291]

Canada

4.208 Canadian legislation does not have a single set of information privacy principles covering both the public and private sectors. Each sector is regulated by its own legislation. The *Privacy Act 1985* (Canada) applies to government institutions, which are defined exhaustively in the Schedule to the Act.[292] The provisions in that Act, which are *not* referred to as principles, cover various stages of the information cycle as it relates to personal information, namely: collection,[293] retention,[294] disposal,[295] use and disclosure[296] and access.[297] The Act also has requirements relating to the inclusion of personal information in personal information banks and the maintenance of personal information indexes.[298]

4.209 There are a number of differences between the IPPs and the provisions in the *Privacy Act 1985* (Canada), some of which have been highlighted in other parts of this chapter. One difference is that, under the Act, a government institution is required expressly to retain personal information that it has used for an 'administrative purpose'[299] for such period of time after it has been used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable

---

289 M Coyle, 'Industry, Government Fret Over Tactics for Fighting Data Theft', *National Law Journal* (online), 10 August 2006, <www.law.com/jlp/nlj>.
290 Ibid. See also Question 11–3(d).
291 N Miller, 'Data Leaks Under Review', *The Sydney Morning Herald* (Sydney), 8 August 2006, 27.
292 See *Privacy Act* RS 1985, c P-21 (Canada) s 3, sch.
293 Ibid ss 4–5.
294 Ibid s 6(1).
295 Ibid s 6(3).
296 Ibid ss 7–9.
297 Ibid ss 12–17.
298 See Ibid ss 10, 11.
299 'Administrative purpose' is defined as a use of personal information in a decision-making process that directly affects the individual. See Ibid s 3.

opportunity to obtain access to the information.[300] The Canadian Act, unlike the IPPs, also imposes an express obligation on government institutions in relation to the disposal of personal information.[301] The Act imposes a lesser test than IPP 10 in relation to the use of personal information for a secondary purpose. While IPP 10 requires that the secondary purpose be 'directly related' to the primary purpose, the Act requires only that the secondary purpose be 'consistent' with the primary purpose.[302] While IPP 6 sets out a high-level and broadly worded right to access personal information, the Canadian Act sets out very detailed and specific rights and procedures in relation to accessing personal information, covering issues such as requests for access, forms of access—including access for persons with a sensory disability—and refusal of access.[303]

4.210 The *Personal Information Protection and Electronic Documents Act 2000* (Canada) (PIPED Act) applies to 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 the organisations.[304] Subject to particular provisions, the 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.[305] The Model Code sets out ten key principles covering: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

4.211 There are a number of differences between the Model Code and the NPPs. For example, the Model Code does not include the principles of identifiers, anonymity and transborder data flows and includes the principle of accountability. Also, while NPP 3 imposes a general requirement on organisations to maintain the quality of personal information, the Model Code provides that personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.[306] It states that 'an organisation shall not routinely update personal information unless such a process is necessary to fulfil the purposes for which the information was collected'.[307]

4.212 Unlike the NPPs, the Model Code elevates consent to a separate principle, stating that:

---

300 Ibid s 6(1).
301 Ibid s 6(3).
302 Ibid s 7(a).
303 Ibid ss 12–17.
304 *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) s 4(1).
305 Ibid s 5.
306 Ibid sch 1, Principle 4.6. This is in line with the approach taken by the Data Quality Principle in the OECD Guidelines. See Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 8.
307 *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) sch 1, Principle 4.6.2.

> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[308]

4.213 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.[309] It provides 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.[310]

4.214 The PIPED Act does not define 'sensitive information'. The Model Code allows an organisation discretion in determining whether information is sensitive.[311]

4.215 Unlike the NPPs and IPPs, the Model Code adopts the related principles of 'accountability' and 'challenging compliance'. The accountability principle provides, in part, that:

> An organisation … shall designate an individual or individuals who are accountable for the organisation's compliance with the [principles]. …[312]
>
> 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.[313]

4.216 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.[314]

4.217 The 'challenging compliance' principle provides, in part, that:

> An individual shall be able to address a challenge concerning compliance with [the principles] to the designated individual or individuals accountable for the organisation's compliance.[315]

---

308 Ibid sch 1, Principle 4.3.
309 See Ibid sch 1, Principles 4.34, 4.36–4.38.
310 Ibid sch 1, Principle 4.36.
311 See Ibid sch 1, Principle 4.34.
312 Ibid sch 1, Principle 4.1.
313 Ibid sch 1, Principle 4.1.3.
314 Ibid sch 1, Principle 4.1.4.
315 Ibid sch 1, Principle 4.10.

4.218 As part of this principle, organisations are obliged to inform individuals who make inquiries or lodge complaints of the existence of complaint procedures, and to investigate all complaints.[316]

Germany

4.219 The *Federal Data Protection Act 1990* (Germany) (FDP Act) does not adopt principles, as such, in protecting personal data in the various stages of the information cycle. However, manifestations of some commonly accepted information privacy principles are reflected in many of it provisions. Some of these provisions have been noted elsewhere in this chapter in the discussion of the IPPs and NPPs. The FDP Act separately regulates the collection, processing,[317] use and disclosure of personal data by public bodies,[318] and by private bodies and commercial public enterprises.[319]

4.220 However, Part I of the FDP Act contains provisions applicable to both the public and private sectors. These provisions cover, for example, consent;[320] transborder data flows;[321] technical and organisational measures to combat unauthorised access to personal data[322]—which is a manifestation of the Security Safeguards Principle in the OECD Guidelines—and the appointment of a data protection officer who is responsible for ensuring that the Act and other provisions concerning data protection are observed[323]—which is a manifestation of the Accountability Principle in the OECD Guidelines.

4.221 Another provision in Part I, entitled 'Data avoidance and data economy', states that:

> 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.[324]

4.222 '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'.[325] Part of this provision is a manifestation of the anonymity principle. However, the German approach to data economy differs from

316 See Ibid sch 1, Principles 4.10.3–4.10.4.
317 'Processing' is defined as the 'storage, modification, communication, blocking and erasure of personal data': *Federal Data Protection Act 1990* (Germany) s 3(4).
318 Ibid pt II.
319 Ibid pt III.
320 Ibid s 4a.
321 Ibid s 4b.
322 Ibid s 9, Annex.
323 Ibid ss 4f, 4g.
324 Ibid s 3a.
325 Ibid s 3(6a).

the IPPs and NPPS insofar as it includes the additional concept of psuedonymisation, and imposes obligations concerning anonymity on public bodies.

4.223 The FDP Act confers a number of rights on the data subject, namely the right to information, the right to correction, erasure or blocking of personal data, and the right to notification. There are separate provisions conferring these rights in a data subject's dealings with public and private bodies.[326] Some of these provisions are manifestations of the Individual Participation Principle in the OECD Guidelines. The right to 'blocking' —which means 'labelling stored personal data so as to restrict their further processing and use'[327]—is not found in the IPPs or NPPs.[328] The FDP Act sets out the circumstances in which personal data are to be blocked, including where:

- preservation periods prescribed by law rule out erasure;
- there is reason to assume that erasure would impair legitimate interests of the data subject;
- erasure is not possible or is only possible with disproportionate effort due to the specific type of storage; or
- in specified circumstances where the data subject disputes that the data are correct and it cannot be ascertained whether or not they are correct.[329]

4.224 Unlike the IPPs, the FDP Act distinguishes between disclosure of data by public bodies to other public bodies,[330] and to private bodies.[331] Disclosure to other public bodies is permitted if it is necessary for the performance of duties of the communicating body or the third party to whom data are disclosed, and the requirements for storage, modification and use of the data are complied with.[332] Disclosure to a private body is permitted if it is necessary for the performance of duties of the communicating body—and other requirements of the Act in relation to storage, modification and use are met—or the private body

326 Ibid ss 19–21, 33–35. See also s 6.
327 See Ibid s 3(4).
328 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(b) provides for a right of blocking of data.
329 See *Federal Data Protection Act 1990* (Germany) ss 20(3), (4) (public bodies), 35(3), (4) (private bodies).
330 Ibid s 15.
331 Ibid s 16.
332 Ibid s 15(1).

> credibly proves a justified interest in knowledge of the data to be communicated and the data subject does not have a legitimate interest in excluding the communication.[333]

4.225 The private sector provisions in the FDP Act contain separate provisions regulating the collection, processing, use and disclosure of data for a private body's own purposes; the collection and recording of data in the course of business with a view to disclosure (for example, for the purposes of marketing, information services, commercial address lists or market research and opinion polling); and the collection and keeping of data in the course of business with a view to disclosure in anonymized form.[334]

United Kingdom

4.226 The *Data Protection Act 1998* (UK) applies to any data controller in respect of data if the data controller is established in the UK, or uses equipment in the UK for processing the data, otherwise than for the purposes of transit through the UK.[335] The Act sets out the following eight data protection principles:

> 1. Personal data shall be processed fairly and lawfully … [336]
>
> 2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
>
> 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
>
> 4. Personal data shall be accurate, and where necessary, kept up to date.
>
> 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
>
> 6. Personal data shall be processed in accordance with the rights of data subjects under this Act.[337]
>
> 7. 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.
>
> 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection

---

333 Ibid s 16(2).

334 See Ibid ss 28–30.

335 *Data Protection Act 1998* (UK) s 5. The Act also binds the Crown. See Ibid s 63.

336 'Processing' means 'obtaining, recording or holding the information or data or carrying out any operation … on the information or data' including use, disclosure, erasure or destruction. See Ibid s 1. This principle extends to the processing of 'general identifiers'. See Ibid sch I pt II cl 4.

337 A person only contravenes this principle by contravening specified sections of the Act that deal with: rights of access to personal data; rights to prevent processing which cause damage or distress; rights to prevent processing for purposes of direct marketing; and rights in relation to automated decision making. See Ibid sch 1 pt II cl 8; ss 7, 10–12.

> for the rights and freedoms of data subjects in relation to the processing of personal data.[338]

4.227 The *Data Protection Act* sets out how some of these principles are to be interpreted.[339] For example, in relation to the first principle, personal data are not to be processed unless one of five conditions specified in Schedule 2 apply. These include where the data subject has given his or her consent to the processing; where the processing is necessary for the performance of a contract to which the data subject is a party; to protect the vital interests of the data subject; for the administration of justice; or where it is necessary

> for the purposes of legitimate interests pursued by the data controller and third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.[340]

4.228 Also in relation to the first principle, the Act prohibits the processing of 'sensitive personal data' unless one of the ten conditions specified in Schedule 3 apply.

4.229 Unlike the principles covered by either the NPPs or IPPs, the UK data protection principles do not cover openness, correction,[341] and anonymity. However, the principles are similar insofar as they cover the areas of collection limitation, data quality, data security, and transborder data flows.

Models to regulate transborder data flows

EU Directive

4.230 In 1998, each of the then 15 member states of the European Union was required to adopt national data protection laws in compliance with the EU Directive, which was formally approved on 24 October 1995.[342] The EU Directive is a detailed document that reflects a series of data protection principles that have been articulated by 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. The Working Party has stated that:

---

338 Ibid sch 1, pt I. Sch 4 sets out the circumstances in which the transborder data flow principle does not apply.

339 See Ibid sch 1 pt II.

340 Ibid sch 2 cl 6(1).

341 Note, however, Ibid s 14, which provides that if a court is satisfied on the application of a data subject that personal data of which the applicant is the subject are inaccurate, the court may order the data controller to rectify, block, erase or destroy those data.

342 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); 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 2006) Ch 14, 8. The EU Directive is discussed further in Ch 13.

> it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate. Such a minimum list should not be set in stone. In some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements.[343]

4.231 The Working Party has stated that the following basic 'content' principles, which are covered in the EU Directive, should be applied:[344]

> 1. **The purpose limitation principle**—data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.[345]
>
> 2. **The data quality and proportionality principle—**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.[346]
>
> 3. **The transparency principle**—individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. … [347]
>
> 4. **The security principle**—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.[348]
>
> 5. **The rights of access, rectification and opposition—**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. …[349]
>
> 6. **Restrictions on onward transfers**—further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (ie the recipient of the onward transfer) is also subject to rules affording an adequate level of protection.[350]

4.232 The Working Party has stated that examples of additional principles to be applied to specific types of processing are:

---

343 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.

344 Ibid. This chapter does not consider the enforcement aspects of the Directive.

345 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 6(b).

346 See Ibid, art 6.

347 See Ibid, arts 10 and 11.

348 See Ibid, art 17.

349 See Ibid, art 12.

350 See Ibid, art 15.

> 1. **Sensitive data**—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.[351]
>
> 2. **Direct marketing**—where data are transferred for 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.[352]
>
> 3. **Automated individual decision**—where the purpose of the transfer 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.[353]

4.233 The EU Directive also introduces the concept of 'legitimate processing', setting out exhaustive grounds pursuant to which personal data lawfully may be processed.[354] In this regard, it goes further than the OECD Guidelines, the IPPs and the NPPs. Grounds for legitimate processing include: where the data subject has 'unambiguously' given his or her consent; where processing is necessary for compliance with a legal obligation to which the data controller is subject; or to protect the vital interests of the data subject.[355]

APEC

4.234 The Asia-Pacific Economic Cooperation Privacy Framework (the APEC Privacy Framework) contains nine privacy principles. The APEC Privacy Framework recognises

> 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.[356]

4.235 The APEC Privacy Framework aims to promote electronic commerce throughout the Asia-Pacific region, and seeks to balance information privacy with business and commercial interests. It also strives to recognise cultural and other diversities within member economies.[357] The APEC Privacy Framework involved 'a conscious effort to build on the OECD Guidelines but to modernise them in light of

---

351 See Ibid, art 8.
352 See Ibid, art 14(b).
353 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.
354 'Processing' includes, for example, collection, recording, storage, retrieval, use and disclosure. 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 2. See also art 7.
355 See Ibid, art 7.
356 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), foreword. The APEC Privacy Framework is discussed in more detail in Ch 13.
357 Ibid, [5]–[6].

more than 20 years' experience and the escalating demand for standards that facilitate multinational data flows'.[358]

4.236 The APEC principles apply to persons or organisations in both the public and private sectors who control the collection, holding, use, transfer or disclosure of personal information.[359]

4.237 The principles cover: preventing harm; notice; collection limitation; use of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability.[360]

4.238 One key difference between the APEC principles and the IPPs and NPPs is that the APEC principles contain separate principles in relation to 'preventing harm', 'choice' and 'accountability'.[361] The prevention of harm principle recognises that one of the primary objectives of the APEC Privacy Framework is to prevent misuse of personal information and consequent harm to individuals. The principle provides that personal information protection should be designed to prevent the misuse of personal information and that remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.

4.239 The APEC principles elevate 'choice' to a separate principle, an approach not taken elsewhere.[362] The 'choice' principle provides that, where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. The principle recognises that it may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.

4.240 Unlike the OECD Guidelines and the EU Directive, the APEC Privacy Framework does not explicitly provide for the principles of transparency and openness. Cate states that the Framework reduces the 'broader goal of transparency' to 'mere notice'.[363]

---

358 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 2006) Ch 14, 11.

359 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [10].

360 See Ibid, [14]–[26].

361 As noted above, the OECD Guidelines also contain an accountability principle.

362 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121. But note discussion above of the principles adopted by the US Federal Trade Commission. A limited subset of the choice principle is found in *Privacy Act 1988* (Cth), sch 3, NPP 8 in relation to anonymity.

363 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 2006) Ch 14, 13. Other criticisms of the APEC principles are raised in Ch 13.

4.241 The APEC principles impose a test similar to that in the OECD Guidelines in relation to allowing the secondary use of personal information when it is for 'compatible or related purposes'.[364] The APEC 'use principle' allows personal information to be used other than for the purposes of collection or compatible or related purposes, 'when necessary to provide a service or product requested by the individual', in addition to the usual exceptions where the individual has given consent or the use is authorised by law.[365]

4.242 Member economies can create local exceptions to the APEC principles, which are not limited by any list of categories.[366] The APEC Privacy Framework provides that any exceptions to the principles, including those relating to national sovereignty, national security, public safety and public policy are to be limited and proportional to meeting the objectives to which the exceptions relate, made known to the public *or* in accordance with law.[367] The use of 'or'—as opposed to 'and'—in this context has been criticised as 'extraordinarily broad'.

> It allows laws authorising secret *classes* of exceptions … and it allows exceptions to be created by a business merely by public notice.[368]

Asia-Pacific Privacy Charter

4.243 The Asia-Pacific Privacy Charter Council (the APPC Council), a regional expert group, has done work on developing 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).[369] The draft APP Charter includes general privacy principles and information privacy principles, which are intended to be observed by both the public and private sectors.[370]

4.244 The general principles cover justification and proportionality, consent, accountability, openness, non-discrimination, and reasons for non-compliance.[371] There are 13 information privacy principles covering: anonymous transactions,[372] collection limitation, identifier limitation, information quality, use and disclosure

---

364 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [19].

365 Ibid, pt III, [19(b)].

366 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121, 123.

367 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

368 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121, 123.

369 See Cyberspace Law and Policy Centre, 'Announcement: Asia-Pacific Privacy Charter Initiative' (Press Release, 1 May 2003).

370 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 11 September 2006.

371 Ibid, Principles 1–6.

372 This principle allows persons to also identify themselves using psuedonyms, where consistent with the nature of the transaction. See Ibid, Principle 7.

limitations, export limitations,[373] access and correction, retention limitation, public registers, information security, automated decisions, identity protection and disclosure of private facts.[374]

4.245 The identifier limitation goes further than the NPPs and IPPs insofar as it prohibits an organisation from *assigning* identifiers to individuals except where necessary for its functions or activities.[375] The APP Charter principles also differ from the NPPs and IPPs insofar as they include principles on public registers, automated decisions, identity protection and disclosure of private facts. The public registers principle provides, in part, that an organisation must not disclose information in a public register unless it is satisfied that the information is to be used for the purpose for which the register is provided, and that organisations and users of public registers must not provide access to the information by methods which are inconsistent with the purpose for which the register is provided.[376]

4.246 The automated decision principle provides that 'an organisation must not make a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human'.[377] The identity protection principle provides that an organisation must take reasonable care not to: (a) allocate identifiers properly allocated to one person to any other person; and (b) deny that any person has the identity or is entitled to use identifiers properly allocated to them.[378] The disclosure of private facts principle provides that 'an organisation must not give publicity to a matter concerning the private life of a person, if the disclosure in extent and content is of a kind that would be seriously offensive and objectionable to a reasonable person of ordinary sensibilities and the organisation knows or ought to know that [fact]'.[379] Differences between the APP Charter and the principles in the APEC Privacy Framework are discussed in Chapter 13.

Question 4–34 Should the *Privacy Act* provide a uniform set of privacy principles that are to apply to both the public (currently covered by the IPPs) and private (currently covered by the NPPs) sectors? If so, what model should be used? Are there any particular principles or exceptions to principles that should apply only to either the public or private sector?

373 The export limitations principle is discussed in Ch 13.

374 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 11 September 2006, Principles 7–19.

375 See Ibid, Principle 9.

376 See Ibid, Principle 15.

377 Ibid, Principle 17.

378 Ibid, Principle 18. This Principle deals with aspects of the problems of identity theft and denial.

379 Ibid, Principle 19.

Question 4–35 Apart from the principles contained in the IPPs and NPPs, are there any other principles to which agencies and organisations should be subject? For example, should the IPPs and NPPs include expressly: an 'accountability' principle; a 'prevention of harm' principle; a 'consent' principle; or a requirement that agencies and organisations notify persons whose personal information has been, or is reasonably believed to have been, accessed without authorisation? If so, what should be the content of these principles?

Level of detail, guidance and protection

4.247 An important issue is whether privacy principles should be detailed or prescriptive or whether they should aim to provide high-level guidance only, which can be supplemented, for example, by guidelines and information sheets issued by the OPC. Existing models of privacy principles vary in the level of detail and guidance that they provide. For example, the OECD Guidelines are pitched at a high-level—they are relatively broad and aspirational—while the Victorian health privacy principles are considerably more detailed and comprehensive.[380]

4.248 An advantage of adopting high-level principles is that it allows for greater flexibility, more easily accommodating unforeseen circumstances and a changing technological environment. The APEC Privacy Framework, expresses the view that the high-level nature of the OECD Guidelines 'makes them still relevant today'.[381] The drawback of adopting 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 principles provide more guidance, thereby promoting certainty and consistency in application. Too much detail can lead to a lack of flexibility.

4.249 The choice about how detailed the principles should be reflects a wider policy choice about the degree to which the regulation of personal information should be 'light-touch'. It is generally harder to establish a breach of a generally worded high-level principle than it is to establish a breach of a principle that imposes detailed and specific obligations. The private sector provisions of the *Privacy Act* introduced what the then Attorney-General called a 'light-touch' co-regulatory approach to information privacy protection, which was intended to be responsive to business and consumer

380 See *Health Records Act 2001* (Vic) sch 1.
381 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), fn 1.

needs.[382] This was to be achieved, in part, by the adoption of high-level principles rather than prescriptive rules.[383]

4.250 Another issue is whether the model to be adopted should aim to achieve a minimum or maximum level of protection of personal information. Alternatively should a standard somewhere between the two extremes be adopted, for example, one that attempts to adopt a best practice approach? Commentators have noted that there are two possible 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 countries progressively weaken their standards to attract global investment in the information technology and services industries.[384]

Question 4–36 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?

382 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General).

383 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 164.

384 C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), xv.

5. Exemptions from the *Privacy Act 1988* (Cth)

Contents

Introduction

5.1 The application of the *Privacy Act 1988* (Cth) is limited by a number of exemptions and exceptions. This Issues Paper refers to *exemptions* where they are independent of specific privacy principles and *exceptions* where they arise under the

Information Privacy Principles (IPPs) or the National Privacy Principles (NPPs).[1] This chapter considers the role of exemptions in general, examines specific exemptions from the *Privacy Act* in the public and private sectors, and canvasses the possibility of new exemptions. Exceptions to the privacy principles are discussed in Chapter 4.

Exemptions under the *Privacy Act*

5.2 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 IPPs, the NPPs (or an approved privacy code), the tax file number provisions or the credit reporting provisions of the Act.

5.3 Broadly speaking, the IPPs apply to acts and practices of Australian Government agencies and the NPPs (or approved privacy codes) apply to acts and practices of private sector organisations.[2] Therefore, entities that fall within the definition of an 'agency' will be bound by the IPPs, and those that fall within the definition of an 'organisation' will be bound by the NPPs (or an approved privacy code).

5.4 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 they are excluded from the definition of 'an act or practice' under s 7 of the Act. For example, while federal courts are within the definition of an 'agency' under the Act, their acts and practices are only covered by the IPPs if they relate to administrative matters.[3]

5.5 Part IIIA of the Act regulates the handling of credit information about individuals by credit reporting agencies and credit providers.[4] 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 from the definition of 'an act or practice' under s 7 of the Act. Credit reporting will be discussed in a separate Issues Paper.

---

1 See 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).

2 *Privacy Act 1988* (Cth) ss 16, 16A.

3 Ibid ss 6(1), 7(1)(a)(ii), (b).

4 A credit reporting agency is a corporation that carries on a credit reporting business: Ibid s 11A. Credit providers include: banks; persons and corporations that operate businesses, where a substantial part of the business is providing loans; retail businesses that issue credit cards; and agencies that carry on businesses involving the making of loans and have been determined by the Privacy Commissioner to be credit providers: *Privacy Act 1988* (Cth) s 11B.

Exemptions under international instruments

OECD Guidelines

5.6 There are no formal 'exemptions' 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).[5] The Guidelines do, however, 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.[6] Acceptable bases for exceptions in the Guidelines include national sovereignty, national security, public policy and the financial interests of the state.[7] Importantly, the Guidelines state that exceptions should be limited to those that are necessary in a democratic society.[8]

5.7 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 different kinds of personal data or in different contexts, for example, credit reporting, criminal investigation and banking.[9]

5.8 The OECD Guidelines also recognise that the application of the Guidelines is subject to various constitutional limitations in federal countries and therefore no commitments exist to apply the Guidelines beyond the limits of constitutional competence.[10]

EU Directive

5.9 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.[11] Examples of exemptions include the processing of data: by a natural person in the course of a purely personal or household activity;[12] 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;[13] for journalistic purposes or the purpose of artistic or

---

5 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).
6 Ibid, Guideline 4.
7 Ibid, Guideline 4; Memorandum, [46].
8 Ibid, Memorandum, [47].
9 Ibid, Memorandum, [19(g)], [47].
10 Ibid, Guideline 5; Memorandum, [48].
11 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).
12 Ibid, art 3(2).
13 Ibid, art 3(2).

literary expression if they are necessary to reconcile the right to privacy with the rules governing freedom of expression.[14]

5.10 Examples of exceptions to the privacy principles in the EU Directive include where the processing is necessary for: the prevention, investigation, detection and prosecution of criminal offences;[15] compliance with a legal obligation;[16] performance of a contract with the data subject;[17] the protection of the vital interests of the data subject;[18] or compilation of data on people's political opinion in the course of electoral activities.[19]

APEC Privacy Framework

5.11 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.[20]

5.12 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.[21] Like the EU Directive, the Framework is not intended to impede governmental activities authorised by law to protect national security, public safety, national sovereignty and other public policy interests.[22] Unlike the EU Directive, the Framework does not contain an exemption for journalistic, literary or artistic expression, or an exception for political or electoral activities.

Issues and problems

Should there be any exemptions from the *Privacy Act*?

5.13 One commentator 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

---

14 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.

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 13(1)(d).

16 Ibid, art 7(c).

17 Ibid, art 7(b).

18 Ibid, art 7(d).

19 Ibid, Recital 36.

20 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

21 Ibid, [10].

22 Ibid, [13].

that privacy protection is entirely lost once a class of organisation or activity is exempted from the privacy principles.[23]

The number of exemptions

5.14 The *Privacy Act* has been criticised for the large number of exemptions it contains.[24] In the public sector, there are more than 20 agencies that are partially or completely exempt from the Act. In the private sector, in addition to the four exempt entities—namely, small business operators, registered political parties, state and territory authorities, and prescribed state and territory instrumentalities—there are 12 categories of acts and practices that are exempt from the Act.

5.15 The OECD Guidelines state that exceptions to the privacy principles should be 'as few as possible'.[25] 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'.[26]

5.16 One commentator has expressed the view that keeping exemptions to a minimum, and limiting them to particular provisions of the law whenever possible, is important to ensure that privacy protection applies as widely as possible throughout the community.[27] 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 these organisations, thus failing adequately to protect the privacy of individuals.[28]

Location of the exemption provisions

5.17 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 *Freedom of*

---

23 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 8 August 2006. Similar views have been expressed in consultations: Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

24 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 8 August 2006; 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.

25 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 4(a).

26 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [13].

27 N Waters, 'Essential Elements of a New Privacy Act' (1999) 5 *Privacy Law & Policy Reporter* 168, 168.

28 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.

Information Act 1982 (Cth) are set out in a schedule to the Act. This has the advantage of clarity as well as reinforcing the message that exemptions are not the primary focus of the legislation.

5.18 One stakeholder was of the view that exemptions should be built into the principles as exceptions, 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.[29]

The scope of exemptions

5.19 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*.[30] 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).[31]

5.20 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 an exception to the exemption. These entities include small business operators, registered political parties, state and territory authorities, and prescribed state and territory instrumentalities.[32] As a result, a large number of entities are exempt from the *Privacy Act*. For example, the 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.[33]

5.21 It has been suggested that blanket exemptions for whole classes of agencies and organisations are undesirable.[34] One commentator has argued that any form of exemption is a very blunt instrument because 'it creates a void within which uncontrolled abuses can occur'.[35]

5.22 It has also been suggested that some of the exemption provisions are expressed too broadly.[36] For example, acts and practices of a media organisation done 'in the

---

29 Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

30 *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 1item 50.

31 *Privacy Act 1988* (Cth) s 6(1).

32 Ibid s 6C(1).

33 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].

34 N Waters, 'Essential Elements of a New Privacy Act' (1999) 5 *Privacy Law & Policy Reporter* 168, 168; G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 1.

35 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 22 August 2006.

36 See, eg, T Dixon, *Government Tables New Privacy Legislation* (2000) AustLII <www.austlii.edu.au/au/other/CyberLRes/2000/6/> at 28 August 2006; Australian Privacy Foundation, *Submission to the*

course of journalism' are exempt from the Act.[37] 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.[38] The terms '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.[39]

Complexity of the exemption provisions

5.23 Some commentators have argued that the exemption provisions in the *Privacy Act* are overly complex.[40] Such complexity makes it difficult to determine the extent to which individuals and entities are exempt from the Act.

5.24 Certain agencies are in effect completely exempt from the operation of the 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', their acts and practices do not fall within the definition of 'an act or practice'.[41] 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.

5.25 The acts and practices of a number of agencies and organisations initially fall outside the definition of 'an act and practice', 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.

5.26 For example, while agencies listed under Schedule 2 Part II Division 1 of the *Freedom of Information Act* fall within the definition of an 'agency', s 7(1)(a)(i)(C) of

---

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.

37 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(4).

38 Ibid s 6(1).

39 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149.

40 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 8 August 2006.

41 *Privacy Act 1988* (Cth) ss 6(1), 7(1)(a)(i)(B).

the *Privacy Act* appears to exempt completely their acts and practices from the definition of an 'act or practice'. However, s 7(1)(c) of the *Privacy Act* then provides that these acts and practices *are* within the definition of 'an act or practice' *except* in relation to records for which the agencies are exempt from the operation of the *Freedom of Information Act*. Further, s 7(2) of the *Privacy Act* provides that provisions in the *Privacy Act except* in respect of the IPPs, the NPPs, an approved privacy code and some of the Privacy Commissioner's functions also apply to these agencies. Finally, s 7A provides that, despite s 7(1)(a)(i), 7(1)(c) and 7(2), acts and practices done in relation to documents in respect of the agencies' commercial activities or the commercial activities of another entity are treated as acts and practices of organisations.

5.27 There has also been criticism about the lack of clarity of some of the exemption provisions.[42] 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.[43]

Question 5–1 Is it appropriate for certain entities to be exempt, either completely or partially, from the operation of the *Privacy Act*? If so, where should the exemptions be located?

Public sector

5.28 The *Privacy Act* prohibits an 'agency' from engaging in an act or practice that breaches the IPPs.[44] Broadly speaking, the term 'agency' refers to those Australian Government entities and persons to whom the IPPs apply. Agencies are not subject to the private sector provisions of the Act unless they have been prescribed by regulation.[45] An agency may also be subject to the tax file number provisions and the credit reporting provisions of the Act in some circumstances.[46]

5.29 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

---

42 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.

43 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.

44 *Privacy Act 1988* (Cth) s 16.

45 Ibid ss 6C, 7A, 16A.

46 Ibid ss 11, 11A, 11B.

Australian Federal Police.[47] The definition of 'agency' excludes incorporated companies, societies and associations even if they are established under Commonwealth law.[48]

5.30 The definition of agency excludes an organisation within the meaning of the *Conciliation and Arbitration Act 1904* (Cth) (now repealed)[49] or a branch of such an organisation.[50] This is a reference to federally registrable employer and employee associations and federally registrable enterprise associations.[51]

5.31 Any act or practice engaged in, 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, engaged in or disclosed to the agency.[52] However, a person is not 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*;[53] or an office established under a Commonwealth or ACT law for the purposes of an agency.[54]

5.32 The following sections consider agencies that are completely or partially exempt from the *Privacy Act*. An agency may be partially exempt where certain acts and practices of the agency fall outside the definition of 'an act or practice' in s 7 of the Act.

Defence and intelligence agencies

Defence Intelligence Group

5.33 The Defence Intelligence Group in the Department of Defence consists of three units: the Defence Imagery and Geospatial Organisation (DIGO), the Defence Signals Directorate (DSD) and the Defence Intelligence Organisation (DIO). These three agencies are exempt from the operation of the *Privacy Act* where their acts and practices relate to their activities.[55] Records that have originated with, or have been received from, these agencies are also excluded from the operation of the Act.[56] Accordingly, agencies and organisations receiving information from these agencies are exempt from the operation of the *Privacy Act* in relation to that information.

---

47 Ibid s 6(1).
48 Ibid s 6(1).
49 The *Conciliation and Arbitration Act 1904* (Cth) was repealed by s 3 of the *Industrial Relations (Consequential Provisions) Act 1988* (Cth).
50 *Privacy Act 1988* (Cth) s 6(1).
51 Workplace Relations Act 1996 (Cth) sch 2 cl 18.
52 *Privacy Act 1988* (Cth) s 8.
53 No such offices have been prescribed under the *Privacy Act 1988* (Cth) or the *Freedom of Information Act 1982* (Cth).
54 *Privacy Act 1988* (Cth) s 6(5).
55 Ibid s 7(1)(ca).
56 Ibid s 7(1)(g).

Furthermore, disclosure of personal information to the DSD is not covered by the Act.[57]

5.34 The DIGO provides intelligence information derived from imagery and other sources in support of Australia's defence and national interests.[58] It is overseen by the Inspector-General of Intelligence and Security (IGIS), who is responsible for ensuring that the DIGO conducts its activities legally, behaves with propriety, complies with any directions from the Minister of Defence and has regard for human rights such as privacy. The Parliamentary Joint Committee on Intelligence and Security also oversees other aspects of the DIGO's operation, including its administration and expenditure. Under s 15 of the *Intelligence Services Act 2001* (Cth), the Minister for Defence is required to make written rules regulating the communication and retention by the DIGO of intelligence information concerning Australians.[59]

5.35 In its Annual Report for 2004–05, the IGIS reported that the scope for collection of imagery by the DIGO that could intrude upon the privacy of Australians was very limited and occurred subject to the *Rules Governing DIGO's Activities in Respect of Australia and Australians*. The IGIS also stated that it planned to assist the DIGO in the development and implementation of new privacy rules.[60]

5.36 The DSD collects and communicates foreign signals intelligence, and provides advice to the Australian Government on the security of information kept in electronic form.[61] Like the DIGO, the DSD is also required to adhere to privacy rules made by the Minister for Defence pursuant to s 15 of the *Intelligence Services Act*. In 2004–05, the IGIS reported that compliance by the DSD with the *Intelligence Services Act* and the associated privacy rules had been satisfactory.[62] In particular, the IGIS reported that the DSD takes its responsibility to comply with the privacy rules seriously and has established a section within the Directorate which is dedicated to monitoring compliance and reporting standards, providing training, and liaising with customers on privacy and related issues.[63]

5.37 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

---

57 Ibid s 7(1A)(c).

58 Australian Government Department of Defence, *Defence Imagery and Geospatial Organisation—About DIGO* <www.defence.gov.au/digo/about.htm> at 10 August 2006.

59 R Hill, *Defence Imagery and Geospatial Organisation Privacy Rules* (2005) Australian Government Department of Defence <www.defence.gov.au/digo/pdf/DIGOprivacyrules.pdf> at 21 July 2006.

60 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2004–2005* (2005), 36, 45.

61 Australian Government Department of Defence, *Defence Signals Directorate—About DSD* <www.dsd.gov.au/about_dsd/index.html> at 9 August 2006.

62 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2004–2005* (2005), iv.

63 Ibid, 30.

making.[64] Unlike the DIGO and DSD, the DIO is not bound by ministerial guidelines in relation to privacy. In its Annual Report for 2004–05, the IGIS stated that it would assist the DIO in the development of privacy rules, with a view to ensuring that the rules are consistent with those in use elsewhere in the Australian intelligence community.[65]

Intelligence agencies

5.38 Under the *Privacy Act*, intelligence agencies are defined to mean ASIO, ASIS and the ONA.[66] Acts and practices of these intelligence agencies are completely exempt from the operation of the *Privacy Act*.[67] A record that has originated with, or has been received from, an intelligence agency is also excluded from the operation of the Act.[68] Accordingly, agencies and organisations receiving information from an intelligence agency are exempt from the operation of the *Privacy Act* in relation to that information. In addition, disclosure of personal information to ASIO or ASIS is not covered by the Act.[69]

5.39 ASIO is Australia's domestic intelligence agency. Its 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.[70] The IGIS can investigate complaints and inquire into compliance by ASIO with the law, ministerial directions and guidelines, propriety and human rights standards.[71]

5.40 Under s 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth), the Minister may give the Director-General of ASIO 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,[72] and another in relation to

64 Australian Government Department of Defence, *Defence Intelligence Organisation* <www.defence.gov.au/dio/index.html> at 10 August 2006.

65 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2004–2005* (2005), 45.

66 *Privacy Act 1988* (Cth) s 6(1).

67 Ibid s 7(1)(a)(i)(B), (2)(a).

68 Ibid s 7(1)(f).

69 Ibid s 7(1A)(a), (b).

70 Australian Security Intelligence Organisation, *About ASIO* <www.asio.gov.au/About/comp.htm> at 10 August 2006; *Australian Security Intelligence Organisation Act 1979* (Cth) s 17.

71 *Inspector-General of Intelligence and Security Act 1986* (Cth) ss 8, 11.

72 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/attorney.htm> at 10 August 2006.

politically motivated violence[73]—both of which set privacy standards for the treatment of personal information. These guidelines are discussed further in Chapter 7.

5.41 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.[74] Section 15 of the *Intelligence Services Act* provides that the responsible Minister in relation to ASIS must make written rules regulating the communication and retention by ASIS of intelligence information concerning Australians.

5.42 The ONA 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.[75] In its 2004–05 Annual Report, the IGIS stated that it will assist the ONA in the development of privacy rules, with a view to ensuring that the rules are consistent with those in use elsewhere in the Australian intelligence community.[76]

Issues

5.43 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'.[77]

5.44 Whether such agencies should continue to be exempt may also depend in part on whether current accountability principles adequately address privacy issues. In the 2004 *Report of the Inquiry into Australian Intelligence Agencies* (Flood Report),[78] it was acknowledged that all elements of government should be accountable. However, the Report stated 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.[79] The Report found that accountability arrangements for the intelligence agencies were

---

73 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/attorney.htm> at 22 July 2006.

74 Australian Secret Intelligence Service, *About ASIS's Role* <www.asis.gov.au/about.html> at 10 August 2006.

75 Australian Government Office of National Assessments, *About Us* <www.ona.gov.au/aboutus.htm> at 19 September 2006.

76 Australian Government Inspector-General of Intelligence and Security, *Annual Report 2004–2005* (2005), 45.

77 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.

78 P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet.

79 Ibid, 51.

working effectively and that the *Intelligence Services Act* has worked well in practice.[80]

5.45 In *Open Government: A Review of the Federal Freedom of Information Act 1982*, 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.[81] They therefore recommended that intelligence agencies remain exempt from the operation of the *Freedom of Information Act*.[82]

5.46 One concern, however, is the lack of privacy rules for the ONA and DIO. As noted above, s 15 of the *Intelligence Services Act* provides that the responsible Ministers in relation to ASIS, DIGO and DSD must make written rules regulating the communication and retention by the relevant agency of intelligence information concerning Australians. ASIO is also required to adhere to privacy guidelines issued by the Attorney-General.[83] However, currently there are no privacy rules applicable to the ONA and DIO.

5.47 The Australian Government has said that as assessors of intelligence collected by others, the activities of the ONA and DIO rarely raise questions of legality and propriety.[84] The Flood Report stated that as assessment agencies, the ONA and DIO do not undertake acts that might interfere with the privacy of Australians. The Report therefore recommended that parliamentary scrutiny of the ONA and DIO should only extend to budgetary and administrative matters and not to the content of the assessments they produce for the Australian Government. The Report stated, however, that the processes by which the ONA and DIO produce their assessments could be open to parliamentary scrutiny.[85] However, these agencies routinely handle potentially sensitive identifying information and this does raise the question of whether they should be subject to certain privacy standards.

Question 5–2 Should the following defence and intelligence agencies be exempt, either completely or partially, from the *Privacy Act*:

- Defence Imagery and Geospatial Organisation;

80 Ibid, 57.
81 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].
82 Ibid, Rec 74.
83 *Australian Security Intelligence Organisation Act 1979* (Cth) s 8A.
84 Commonwealth, *Parliamentary Debates*, House of Representatives, 22 May 1986, 3703 (L Bowen—Attorney-General).
85 P Flood, *Report of the Inquiry into Australian Intelligence Agencies* (2004) Australian Government Department of Prime Minister and Cabinet, 58.

- Defence Intelligence Organisation;
- Defence Signals Directorate;
- Australian Security Intelligence Organisation;
- Australian Secret Intelligence Service; and
- Office of National Assessments?

If so, what is the policy justification for the exemption? Are there any other defence and intelligence agencies that should be exempt, either completely or partially, from the *Privacy Act*?

Agencies other than defence and intelligence agencies

Ministers

5.48 The *Privacy Act* applies to Australian Government ministers only where their acts and practices relate to the affairs of agencies, 'eligible case managers'[86] or 'eligible hearing service providers';[87] or where the acts and practices are in relation to a record concerning these affairs that is in the ministers' possession in their official capacity.[88] Other acts and practices of ministers are exempt from the operation of the Act.[89]

Federal courts

5.49 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[90]—fall within the definition of 'agency' in the *Privacy Act*.[91] Acts and

86 The 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.

87 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).

88 *Privacy Act 1988* (Cth) s 7(1)(d)–(ed).

89 Ibid s 7(1)(a)(iii).

90 The Industrial Relations Court of Australia is also a federal court. However, as a consequence of the *Workplace Relations and Other Legislation Amendment Act 1996* (Cth), the court's jurisdiction has been transferred to other courts. Despite the transfer of jurisdiction, the Industrial Relations Court continues to

practices of the federal courts in relation to their administrative records—including personnel records, operations and financial records, freedom of information (FOI) records, complaint files and mailing lists—are covered by the *Privacy Act*.[92] 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.[93]

5.50 The partial exemption of federal courts from the *Privacy Act* reflects a balance between the protection of individual privacy and the principle of open justice. Public access to court proceedings is vital to maintaining public confidence in the administration of justice.[94] Privacy issues arise 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.[95]

5.51 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.[96] Court judgments containing sensitive personal information may be recorded in law reports and computerised legal databases and become available to the public.[97] Other case information, such as correspondence between the courts and the parties, is generally not in the public arena but is kept on file in court registries.

Public access to court records

5.52 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, family law, bankruptcy and criminal proceedings. In addition,

---

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 19 September 2006.

91 *Privacy Act 1988* (Cth) s 6(1).

92 Ibid s 7(1)(b); *I v Commonwealth Agency* [2005] PrivCmrA 6.

93 *Privacy Act 1988* (Cth) s 7(1)(a)(ii); *I v Commonwealth Agency* [2005] PrivCmrA 6.

94 *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.

95 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 54.

96 Ibid, 55.

97 In *Le and Secretary, Department of Education, Science and Training* (2006) 90 ALD 83, the Administrative Appeals Tribunal 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.

children are considered to be particularly vulnerable and therefore the identification of children in court records raises specific privacy concerns.[98]

5.53 Although exempt from the *Privacy Act*, access to documents on file in court registries is regulated by other statutes or rules of court.[99] For example, 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.[100] A person who is not a party to the proceeding may only inspect certain other documents with the leave of the court.[101] Leave will usually be granted, however, where a document has been admitted into evidence or read out in open court.[102]

Media access to court records

5.54 Media reports are how most members of the public gain access to 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.

5.55 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 … [103]

5.56 However, some legislation 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 cannot 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.

---

98 The identification of children in court records is discussed in Ch 9.

99 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.

100 *Federal Court Rules 1979* (Cth) o 46 r 6(1), (2).

101 Ibid o 46 r 6(3)–(5).

102 Federal Court of Australia, *Public Access to Court Documents* <www.fedcourt.gov.au> at 21 July 2006.

103 *Raybos Australia Pty Ltd v Jones* (1985) 2 NSWLR 47, 55, 58.

Research access to court records

5.57 Research access may be considered an aspect of open justice because 'research offers a more considered and sustained evaluation of the way courts operate'.[104] 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 cases, show that they have a proper interest in searching court records and inspecting court documents.[105]

5.58 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.[106] 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 fully articulated and published.[107]

Party and witness access to court records

5.59 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.[108]

5.60 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 FOI and privacy legislation gives individuals the right to correct information held about them in public records, the same rule should apply to court records.[109]

Some options for reform

5.61 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*, 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;

---

104 C Puplick, 'Justice: Now Open to Whom?' (2002) 6 *Judicial Review* 95, 105.
105 See, eg, *Federal Magistrates Court Rules 2001* (Cth) r 2.08(2).
106 County Court of Victoria, *Discussion Paper: Access to Court Records* (2005), [28].
107 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), [8.40], Rec R27.
108 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 55.
109 Ibid, 55.

whether leave of the court is required for access; and the release of transcripts to non-parties.[110] 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.[111]

5.62 Inquiries in other jurisdictions have recommended the consolidation of legislative provisions concerning access to court records, either in criminal and civil procedure legislation,[112] or in separate legislation dealing specifically with court information.[113]

5.63 In its discussion paper, *Review of the Policy on Access to Court Information*,[114] the Attorney General's Department of New South Wales has proposed a system whereby court information is classified as either open to public access or restricted public access.[115] 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.[116] Restricted access information would also be subject to the provisions of the *Privacy and Personal Information Protection Act 1998* (NSW).[117]

5.64 The County Court of Victoria has also released a discussion paper on access to court records.[118] The Court's proposals include that: applications by the media for the release of information from court proceedings be made to the trial judge, before or during the trial;[119] non-party access to civil files generally be available unless the court orders otherwise;[120] 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;[121] and no access to criminal or appeal files by non-parties without an order of the court.[122]

---

110 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [7.25], [7.36].
111 Ibid, Rec 7–1. This recommendation has not yet been implemented.
112 New South Wales Government Attorney General's Department, *Review of the Policy on Access to Court Information* (2006), Proposal 1.
113 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), Rec R6.
114 New South Wales Government Attorney General's Department, *Review of the Policy on Access to Court Information* (2006).
115 Ibid, Proposal 3.
116 Ibid, Proposal 7.
117 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.
118 County Court of Victoria, *Discussion Paper: Access to Court Records* (2005).
119 Ibid, [12].
120 Ibid, [14], [16].
121 Ibid, [18].
122 Ibid, [20].

5.65 In its report on access to court records, 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,[123] including the protection of sensitive, private or personal information.[124]

5.66 Another way that an appropriate balance between the interests of open justice and privacy may be achieved is by removing certain identifying information from court 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.[125] In September 2003, the Judicial Conference further permitted remote public access to electronic criminal case files (with certain exceptions) if specified personal identifiers were edited.[126] Electronic access to court records is discussed further in Chapter 11.

5.67 One commentator has suggested four options for reform in relation to court records. One option is to require courts to comply with the IPPs, but with narrowly defined exemptions to protect the actual hearing process. Alternatively, court records could be categorised according to levels of access, although this might be an administratively complex process. A third option is to require digital signature or registration before giving people access to court files. A final option is to anonymise cases, which could be re-linked with the identified subjects where there was a public interest in identities being known.[127]

Industrial tribunals

5.68 Industrial tribunals listed in Schedule 1 to the *Freedom of Information Act* are exempt from the *Privacy Act* except in relation to administrative matters.[128] These tribunals include the Australian Industrial Relations Commission (AIRC), the

123 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), Rec R6.

124 Ibid, Rec R11.

125 However, social security cases are to be excluded 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 2006.

126 Judicial Conference of the United States, *Judicial Privacy Policy Page* <www.privacy.uscourts.gov> at 14 August 2006. 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.

127 C Puplick, 'How Far Should the Courts be Exempted from Privacy Regulation?' (2002) 40(5) *Law Society Journal* 52, 55–56.

128 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(A), (b).

Australian Fair Pay Commission, and the Industrial Registrar and Deputy Industrial Registrars.

5.69 Other federal tribunals, such as the Administrative Appeals Tribunal, the Migration Review Tribunal, the Refugee Review Tribunal and the Social Security Appeals Tribunal, are covered by the *Privacy Act*. Although these tribunals are not industrial or conciliatory bodies, they perform quasi-judicial functions and may therefore have a similar claim to exemption as federal courts. The ALRC is interested in views on whether any federal tribunals other than the industrial tribunals should also be exempt, either completely or partially, from the *Privacy Act*.

Australian Crime Commission

5.70 The Australian Crime Commission (ACC) was established under the *Australian Crime Commission Act 2002* (Cth) to counter serious and organised crime. The functions of the ACC include collecting and analysing criminal intelligence; setting national criminal intelligence priorities; and conducting intelligence-led investigations into federally relevant criminal activity.[129]

5.71 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'.[130] In addition, s 7(2) of the Act exempts the ACC from compliance with the tax file number provisions of the Act. Therefore, the ACC is completely exempt from the operation of the Act.

5.72 Furthermore, acts and practices in relation to records that have originated with, or have been received from, the ACC or the Board of the ACC are also exempt.[131] Accordingly, agencies and organisations receiving information from the ACC are exempt from the operation of the *Privacy Act* in relation to that information.

5.73 It has been said that there is a fundamental tension between the interests of privacy and the interests of 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.[132]

---

129 Australian Crime Commission, *Australian Crime Commission Profile—Dismantling Serious and Organised Criminal Activity* (2005) <www.crimecommission.gov.au/content/about/ACC_PROFILE.pdf> at 9 August 2006.

130 *Privacy Act 1988* (Cth) s 7(1)(a)(iv).

131 Ibid s 7(1)(h).

132 C Corns, 'Inter Agency Relations: Some Hidden Obstacles to Combating Organised Crime?' (1992) 25 *Australia and New Zealand Journal of Criminology* 169, 177.

Royal commissions

5.74 Federal royal commissions are government inquiries established by the Governor-General pursuant to the *Royal Commissions Act 1902* (Cth). While royal commissions fall within the definition of an 'agency', their acts and practices are excluded from the definition of 'an act or practice' and therefore from the operation of the *Privacy Act*.[133]

5.75 Privacy concerns have been raised where inquiries by royal commissions are held in public. One commentator has argued 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.[134]

Integrity Commissioner

5.76 In June 2006, the Australian Commission for Law Enforcement Integrity was established to detect and investigate corruption in the Australian Federal Police, the ACC, the former National Crime Authority and prescribed Australian Government agencies with law enforcement functions.[135] It is headed by the Integrity Commissioner who has similar powers to a royal commission, including the power to: execute search warrants; conduct public or private hearings; summon people to attend hearings to give evidence or produce documents or things; and take possession of, copy or retain any document or thing.[136] The functions of the Integrity Commissioner 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.[137]

5.77 The *Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006* (Cth), once commenced, will exempt the acts and practices of the Integrity Commissioner from the operation of the *Privacy Act*.[138] Acts and practices in relation

---

133 *Privacy Act 1988* (Cth) s 7(1)(a)(v).

134 M Rayner, 'Commissions and Omissions' (1996) 6(10) *Eureka Street* 14.

135 *Law Enforcement Integrity Commissioner Act 2006* (Cth) ss 5(1) (definition of 'law enforcement agency'), 7, 15. No Australian Government agencies have yet been prescribed under the Act.

136 Ibid pt 9.

137 Ibid s 15.

138 *Law Enforcement Integrity Commissioner (Consequential Amendments) Act 2006* (Cth) sch 1 item 50 will amend the *Privacy Act* to exclude the acts and practices of the Integrity Commissioner from the definition of an 'act or practice' in the *Privacy Act*. The *Law Enforcement Integrity Commissioner (Consequential*

to a record that has originated with, or has been received from, the Integrity Commissioner or a staff member of the Australian Commission for Law Enforcement Integrity, will also be exempt from the *Privacy Act*.[139]

Schedule 2 Part I Division 1 of the Freedom of Information Act

5.78 Certain agencies listed in Schedule 2 Part I Division 1 of the *Freedom of Information Act*—including Aboriginal Land Councils and Land Trusts, the Auditor-General, the IGIS, and the National Workplace Relations Consultative Council—are exempt from compliance with the IPPs.[140] However, other provisions of the Act, such as the tax file number provisions, do apply to these agencies.

5.79 The intelligence agencies—ASIO, ASIS and ONA[141]—are also listed in Schedule 2 Part I Division 1 of the *Freedom of Information Act*. As discussed above, however, these agencies are completely exempt from the *Privacy Act*.[142]

5.80 Section 7A of the *Privacy Act* provides for agencies listed in Schedule 2 Part I of the *Freedom of Information Act* to be treated as organisations by regulation. Where an agency has been prescribed by regulation for this purpose, the NPPs or approved privacy code will apply. Currently the only prescribed agencies are the Australian Government Solicitor and the Australian Industry Development Corporation.[143]

5.81 Aboriginal Land Councils and Land Trusts were exempted from the *Freedom of Information Act* because they were separate from the executive arm of the government and therefore not subject to public sector responsibilities.[144] 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.

5.82 The Auditor-General is an independent statutory officer responsible for auditing the activities of most Commonwealth public sector entities. The Auditor-General has broad information-gathering powers and authority to have access to Commonwealth

---

Amendments) Act was assented to on 30 June 2006. At the time of writing, the relevant statutory provision has not yet commenced.

139 Ibid sch 1 item 51. At the time of writing, this statutory provision has not yet commenced.

140 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2).

141 Ibid s 6(1).

142 Ibid s 7(1)(a)(i)(B), (2)(a).

143 *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). However, due to some long term obligations, the winding down of the Australian Industry Development Corporation is unlikely to be fully complete before 2010: Australian Industry Development Corporation, *Statement of Intent* <www.finance.gov.au/gbpfau/> at 21 August 2006.

144 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

premises.[145] 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.[146]

5.83 The National Workplace Relations Consultative Council—established under the *National Workplace Relations Consultative Council Act 2002* (Cth)—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.[147] In its review of the Freedom of Information Bill 1978 (Cth), the Senate Standing Committee on Constitutional and Legal Affairs did not consider that the Council should 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.[148]

5.84 The 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) 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. It regularly monitors the activities of certain intelligence and security agencies, conducts inquiries, investigates complaints about these agencies, makes recommendations to the government and provides annual reports to the Australian Parliament.[149]

5.85 During parliamentary debate in the House of Representatives 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.[150] Particular

---

145 *Auditor-General Act 1997* (Cth) pt 5 div 1.

146 Ibid s 36.

147 *National Workplace Relations Consultative Council Act 2002* (Cth) s 5.

148 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].

149 Inspector-General of Intelligence and Security, *Frequently Asked Questions* <www.igis.gov.au/faq's.cfm> at 22 July 2006.

150 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.

mention was made of the Aboriginal Land Councils and Land Trusts, the Auditor-General and the National Labour Consultative Council.[151]

5.86 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.[152] The ALRC and ARC recommended that all agencies listed in Schedule 2 Part I of the *Freedom of Information Act* (other than the intelligence agencies and government business enterprises) should be required to demonstrate to the Attorney-General the grounds on 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.[153]

5.87 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 *Freedom of Information 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 *Freedom of Information Act*.[154]

5.88 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 *Freedom of Information Act* should be examined more closely before amending the legislation.[155] The Bill was amended to remove the proposal.

Schedule 2 Part II Division 1 of the Freedom of Information Act

5.89 A number of Australian Government agencies listed under Schedule 2 Part II Division 1 of the *Freedom of Information Act* are exempt from the *Privacy Act* where their acts and practices relate to documents specified in the *Freedom of Information Act* to the extent that those documents relate to the non-commercial activities of the agencies or of other entities.[156] In relation to documents that are *not* specified under the

---

151 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.

152 Australian Law Reform Commission and Administrative Review Council, *Freedom of Information*, IP 12 (1994), [12.4].

153 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.

154 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].

155 Ibid, [3.137].

156 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

Freedom of Information 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.[157] These agencies are also covered by the NPPs where their acts and practices relate to commercial activities or to documents concerning commercial activities.[158] In addition, they are required to comply with the tax file number provisions and, where applicable, the credit reporting provisions of the *Privacy Act*.[159] These agencies are described below.

Financial departments and agencies

5.90 The Department of the Treasury focuses primarily on economic policy and has three policy objectives—effective government spending and taxation arrangements, sound macroeconomic environment, and well functioning markets.[160] 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.[161]

5.91 The Australian Transaction and Analysis Centre (AUSTRAC) is Australia's anti-money laundering 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) 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 and revenue agencies.[162] The acts and practices of AUSTRAC are exempt where they relate to documents concerning information communicated to it under s 16 of the *Financial Transaction Reports Act*—the reporting of suspected illegal transactions.[163]

5.92 The Reserve Bank of Australia is a statutory authority, with responsibilities for formulating and implementing monetary policy, maintaining financial system stability, 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.[164] The acts and practices of the Reserve Bank are exempt where they relate to documents concerning its banking operations (including individual open market operations and foreign exchange

157 Ibid s 7(1)(c).
158 Ibid s 7A.
159 Ibid s 7(2).
160 Australian Government—The Treasury, *About Treasury* <www.treasury.gov.au> at 11 August 2006.
161 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.
162 AUSTRAC, *About AUSTRAC* <www.austrac.gov.au> at 10 August 2006.
163 *Privacy Act 1988* (Cth) s 7(1)(c).
164 Reserve Bank of Australia, *About the RBA* <www.rba.gov.au/AboutTheRBA/> at 10 August 2006.

dealings) or exchange control matters, to the extent that these documents relate to non-commercial activities.[165]

5.93 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.[166] The acts and practices of the Corporation are exempt where they 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.[167]

Statutory media agencies

5.94 The Australian Communications and Media Authority (ACMA) is a statutory body responsible for the regulation of broadcasting, radiocommunications, telecommunications and online content. Its responsibilities include: promoting self-regulation and competition in the telecommunications 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, including the broadcasting services bands; and representing Australia's communications and broadcasting interests internationally.[168]

5.95 The Classification Board and the Classification Review Board are separate and independent statutory bodies. The Classification Board meets on a regular basis to classify films (including videos and DVDs), computer games and certain publications before they are made available to the public.[169] 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.[170]

5.96 The Office of Film and Literature Classification is an agency within the Attorney-General's portfolio that provides administrative support to the Classification Board and the Classification Review Board. It processes applications, provides services

---

165 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

166 Australian Government Export and Finance Insurance Corporation, *About Us* <www.efic.gov.au> at 10 August 2006.

167 *Privacy Act 1988* (Cth) ss 7(1)(c), 7A.

168 Australian Communications and Media Authority, *About ACMA* <www.acma.gov.au/acmainter> at 10 August 2006.

169 Australian Government Office of Film and Literature Classification, *The Classification Board* <www.oflc.gov.au/special.html?n=250&p=58> at 10 August 2006.

170 Australian Government Office of Film and Literature Classification, *The Classification Review Board* <www.oflc.gov.au/special.html?n=251&p=62> at 10 August 2006.

to the Office's clients and the community, offers classification training programs and develops classification policy.[171]

5.97 These agencies are exempt from the *Privacy Act* where their acts and practices concern 'exempt Internet-content documents' under Schedule 5 to the *Broadcasting Services Act 1992* (Cth).[172]

National broadcasters

5.98 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.[173]

5.99 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.[174]

5.100 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.[175] However, s 7A of the Act provides 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. 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.[176] Therefore, to the extent that program materials and datacasting content of the ABC and SBS relate to commercial activities, they are

---

171 Australian Government Office of Film and Literature Classification, *The Office of Film and Literature Classification* <www.oflc.gov.au/special.html?n=252&p=204> at 10 August 2006.

172 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: *Freedom of Information Act 1982* (Cth) s 4(1).

173 *Australian Broadcasting Corporation Act 1983* (Cth) s 6.

174 *Special Broadcasting Service Act 1991* (Cth) s 6.

175 'Datacast' means to broadcast digital information: *Macquarie Dictionary* (online ed, 2005). 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.

176 *Privacy Act 1988* (Cth) s 7A.

covered by the private sector provisions of the *Privacy Act*. 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.[177] The exemption relating to journalism is discussed further below.

Austrade

5.101 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.[178] Austrade is exempt from the *Privacy Act* in relation to documents concerning the carrying out of overseas development projects, to the extent that these documents relate to non-commercial activities.[179]

National Health and Medical Research Council

5.102 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 health standards between the various states and territories, fostering health and medical research and training, and monitoring ethical issues relating to health throughout Australia.[180] The acts and practices of NHMRC are exempt from the *Privacy Act* where they relate to documents in the possession of its 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.

Question 5–3 Should the following agencies be exempt, either completely or partially, from the *Privacy Act*:

- Australian Government ministers;
- federal courts;

177 Ibid ss 7(1)(ee), 7B(4).
178 Austrade, *Organisation Overview* <www.austrade.gov.au/> at 10 August 2006.
179 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).
180 National Health and Medical Research Council, *Role of the NHMRC* <www.nhmrc.gov.au/about/role/index.htm> at 10 August 2006.

- agencies specified in Schedule 1 to the *Freedom of Information Act 1982* (Cth)—namely, the Australian Industrial Relations Commission, the Australian Fair Pay Commission, the Industrial Registrar and Deputy Industrial Registrars;
- Australian Crime Commission;
- royal commissions;
- Integrity Commissioner;
- agencies specified in Schedule 2 Part I Division 1 of the *Freedom of Information Act* 1982 (Cth) other than the intelligence agencies, the Australian Government Solicitor and the Australian Industry Development Corporation; and
- agencies specified in Schedule 2 Part II Division 1 of the *Freedom of Information Act 1982* (Cth)?

If so, what is the policy justification for the exemption? Are there any other agencies that should be exempt, either completely or partially, from the *Privacy Act*?

State and territory authorities and prescribed instrumentalities

5.103 State and territory authorities fall outside the definition of 'agency' and are also specifically excluded from the definition of 'organisation' under the *Privacy Act*.[181] Therefore they are exempt from the operation of the Act unless states and territories request that such authorities be brought into the regime by regulation.[182] 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 established for a public purpose under a state or territory law.[183]

5.104 State and territory statutory corporations are excluded from the coverage of the *Privacy Act*.[184] However, state and territory bodies that are incorporated companies, societies or associations are deemed to be 'organisations' for the purposes of the Act.[185] They can be prescribed out of the coverage of the Act, but only on request by

181 *Privacy Act 1988* (Cth) ss 6(1), 6C.
182 Ibid s 6F.
183 Ibid s 6C(3).
184 Ibid s 6C(3)(c).
185 Ibid s 6C(1), (3)(c)(i).

the relevant state or territory and only after the Minister has considered a number of issues outlined in the Act.[186]

5.105 State and territory instrumentalities also fall outside the definition of 'agency' under the *Privacy Act*. However, they are 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.

5.106 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.[187] 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.[188]

5.107 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.[189]

5.108 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.[190]

5.109 Some state and territory instrumentalities are required by other federal legislation to comply with the *Privacy Act*. For example, 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 purposes of the provision of financial assistance to students.[191] One higher education provider

---

186 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.

187 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [73].

188 Ibid, notes on clauses [74].

189 Ibid, notes on clauses [96].

190 *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).

191 *Higher Education Support Act 2003* (Cth) s 19-60.

submitted that the *Higher Education Support Act* does not necessarily enforce a universal approach to privacy and may not be consistent with state and territory privacy principles. It submitted that the application of one set of privacy principles throughout Australia would assist implementation and enforcement of the Act.[192]

5.110 For the period from 21 December 2001 to 31 January 2005, the Office of the Privacy Commissioner (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.[193] 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*.[194]

5.111 Submissions to the inquiry by the Senate Legal and Constitutional References Committee into the *Privacy Act* (2005 Senate Committee privacy inquiry) have argued that the exemption in relation to state agencies is a significant gap in the coverage of the *Privacy Act*.[195] In addition, a number of stakeholders have queried whether it is appropriate for certain state and territory statutory bodies to fall outside both the federal and the state privacy regimes.[196]

5.112 Another issue raised in consultation is 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.[197] This issue is discussed further in Chapter 7.

5.113 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 2.

Question 5–4 Should state and territory authorities be exempt from the privacy principles in the *Privacy Act*?

192 D Antulov, *Submission PR 14,* 28 May 2006.
193 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.
194 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 38.
195 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.38]. This view was also expressed in a consultation in this Inquiry: Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.
196 Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006; Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006.
197 G Hill, *Consultation PC 21*, Melbourne, 8 May 2006.

Question 5–5 In addition to the energy distributors owned by the New South Wales Government, which are the only state authorities prescribed under the *Privacy (Private Sector) Regulations 2001* (Cth), are there any other state or territory authorities that should be covered by the privacy principles in the *Privacy Act*? If so, to what extent should they be covered?

Government contractors and subcontractors

Organisations acting under a Commonwealth contract

5.114 Australian Government agencies that outsource functions involving the collection or holding of personal information are required to take contractual measures to ensure that their contractors or subcontractors do not breach the IPPs and that the contracts do not authorise such a breach.[198]

5.115 Under the *Privacy Act*, a contract between an Australian Government agency and a contractor—or between a contractor and any subcontractor—is to be the primary source of the contractor's obligations in relation to the personal information dealt with for the purpose of performing the contract.[199] Under ss 6A(2) and 6B(2) of the *Privacy Act*, acts and practices of a government contractor acting under a Commonwealth contract do not breach the NPPs or approved privacy codes if they are authorised by a contractual provision dealing with privacy that is inconsistent with the NPPs or the codes.[200] However, acts and practices by these contractors may be an interference with privacy if they are inconsistent with that contractual provision.[201]

5.116 Many small businesses are exempt from the *Privacy Act*. Under s 6D of the Act, however, Commonwealth contractors are excluded from the definition of small business operators.[202] Therefore a small business may be subject to the Act in respect of the performance of the contract, but will be exempt in relation to acts and practices that are for other purposes.[203]

5.117 The Act also protects personal information held by government contractors for the purposes of a Commonwealth contract from being used for direct marketing purposes unrelated to the contract itself.[204]

---

198 *Privacy Act 1988* (Cth) s 95B.

199 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 7. See also Office of the Federal Privacy Commissioner, *Privacy Obligations for Commonwealth Contracts*, Information Sheet 14 (2001), 1.

200 These provisions do not apply to government agencies of the ACT and their contractors: Office of the Federal Privacy Commissioner, *Privacy Obligations for Commonwealth Contracts*, Information Sheet 14 (2001), 1.

201 *Privacy Act 1988* (Cth) s 13A(1)(c).

202 Ibid s 6D(4)(e). The small business exemption is discussed in detail below.

203 Ibid s 7B(2).

204 Ibid ss 13A(1)(d), 16F.

5.118 Submissions to the review by the OPC of the private sector provisions of the *Privacy Act* (OPC Review) raised a number of issues concerning the application of both the IPPs and NPPs to Australian Government contractors, including: uncertainty about the obligations that apply when a contractor deals with personal information on behalf of an Australian Government agency; and compliance with both set of principles is unreasonably burdensome on community sector organisations and may impede unnecessarily the provision of Australian Government funded health services.[205] Similar concerns also were raised with the 2005 Senate Committee privacy inquiry. Submissions to that inquiry noted that Australian Government contractors may have to comply with three sets of principles: the NPPs, the IPPs and any applicable state or territory privacy laws, and that the application of these requirements is complex and confusing.[206] In consultations in this Inquiry, some stakeholders expressed similar views,[207] especially where a project involves joint government funding arrangements at both state and federal levels.[208]

5.119 The OPC commented that the lack of consistency between the IPPs and the NPPs has caused considerable compliance difficulties for Australian Government contractors.[209] For this reason, the OPC recommended that the Australian Government consider commissioning a systematic examination of both the IPPs and the NPPs with a view to developing a single set of privacy principles that would apply to both agencies and organisations.[210] This is discussed in detail in Chapter 4.

Organisations acting under a state contract

5.120 Contactors and subcontractors to state and territory authorities are exempt from the operation of the *Privacy Act* where they are acting under a state or territory contract.[211] The purpose of this exemption is to ensure that

> private sector organisations providing services under contract to a State or Territory authority are exempt from the Commonwealth's privacy regime in respect of those services and can be regulated by the relevant State or Territory.[212]

5.121 However, state and territory privacy regimes vary significantly in terms of their coverage of contractors acting under state and territory contracts. Currently, state

---

205 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 39.

206 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.78]–[5.79].

207 A MacRae, *Consultation PC 31*, Melbourne, 5 July 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006.

208 Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006.

209 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 46.

210 Ibid, Rec 5.

211 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(5).

212 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [113].

contractors are only covered by privacy regimes in New South Wales, Victoria, Tasmania and the Northern Territory.[213] In Queensland, South Australia, Western Australia, and the ACT, state contractors are not covered by the state privacy regimes. Even where there is an applicable state or territory privacy regime, certain acts that do not fall plainly within the state contract may not be covered by the state or territory regime.

5.122 Issues concerning organisations that provide contracted services involving personal information to Australian Government and state or territory agencies are discussed further in Chapter 7.

Private sector

5.123 While the IPPs bind public sector agencies, the NPPs bind private sector entities that fall within the definition of an 'organisation'. An 'organisation' is defined as an individual, a body corporate,[214] a partnership,[215] any other unincorporated association[216] or a trust[217] that is not exempt from the operation of the *Privacy Act*.[218] 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.[219]

5.124 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:

- what constitutes a breach of the NPPs or an approved privacy code;

---

213 *Privacy and Personal Information Protection Act 1998* (NSW) s 9; *Information Privacy Act 2000* (Vic) s 9(1)(j); *Information Act 2002* (NT) s 7(c).

214 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.

215 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.

216 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.

217 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.

218 *Privacy Act 1988* (Cth) s 6C.

219 Ibid s 6C.

- what constitutes an interference with the privacy of an individual;
- the definition of an act or practice; or
- the operation of the Act.

5.125 Some of the private sector exemptions under the *Privacy Act* are not contained in the OECD Guidelines, the EU Directive or the APEC Privacy Framework—for example, the exemptions for small business operators and employee records. The following sections examine specific exemptions from the *Privacy Act* that apply to the private sector.

Small business operators

5.126 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 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.[220]

5.127 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).[221] 'Small businesses' can include non-profit bodies and unincorporated associations,[222] even though the ordinary meaning of the term 'business' may not include such bodies. There are a number of exceptions to 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;[223]
- trades in personal information (unless it always has the consent of the individuals concerned, or only does so when authorised or required by law);[224]

---

220 Ibid s 6D(3).

221 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 20 June 2006.

222 Office of the Privacy Commissioner, *A Snapshot of the Privacy Act for Small Business* <www.privacy.gov.au/business/small/bp.html> at 31 August 2006.

223 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 19 June 2006.

224 *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 20 June 2006.

- 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.[225]

5.128 The Attorney-General may prescribe that certain small businesses or their activities be subject to the Act despite the exemption. The Attorney-General may do so if it is in the public interest and after consultation with the Privacy Commissioner.[226] 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.[227]

5.129 The Commissioner keeps a register of those businesses that choose to 'opt in'. Currently there are 147 small businesses that have opted to be covered by the *Privacy Act*.[228]

5.130 Small businesses were exempted on the basis that many of them do not pose a high risk to privacy.[229] 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 interests.[230] It was also the policy of the Australian Government to minimise compliance costs on small businesses.[231] The exceptions to 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.[232]

5.131 The OPC indicated that for the period from 21 December 2001 to 31 January 2005, 20% of all the NPP complaints closed by the Office as outside of its jurisdiction concerned the small business exemption.[233] In 2004–05, the OPC received 2,469

---

225 *Privacy Act 1988* (Cth) ss 6D(4), (9), 6E, 6EA.
226 Ibid s 6E(4).
227 Australian Government Attorney-General's Department, *Fact Sheet on Privacy in the Private Sector—Small Business* (2000) <www.ag.gov.au> at 19 June 2006.
228 Office of the Privacy Commissioner, *Opting-In to Coverage by the National Privacy Principles* <www.privacy.gov.au/business/register/index.html> at 20 June 2006.
229 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 6.
230 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams—Attorney-General), 22370–22371.
231 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 6.
232 Ibid, 6.
233 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

enquiries concerning exemptions, of which 17% relate to the small business exemption.[234]

Retention or removal of the exemption

5.132 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)[235] and the Senate Legal and Constitutional Legislation Committee inquiry (2000 Senate Committee inquiry).[236]

5.133 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 overly burdening small businesses that pose a low privacy risk, and that this cannot be achieved without some form of exemption for small businesses.[237] The 2000 Senate Committee inquiry recommended the retention of the exemption, on the basis that it 'achieve[s] an adequate balance between concerns about the coverage of the exemption and the intention not to impose too great a burden on small businesses'.[238]

5.134 In 2005, both the OPC and the Senate Legal and Constitutional References Committee reviewed the private sector provisions of the *Privacy Act*.[239] Submissions to the OPC Review were roughly divided between retention of the small business exemption and its repeal.[240] In evidence before the 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

234 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 38.

235 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000).

236 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000).

237 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].

238 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].

239 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).

240 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 180.

> entirely, there would be a cost to I think it is 1.2 million small businesses in Australia.[241]

The Privacy Commissioner acknowledged, however, that the OPC had not assessed the estimated cost of removing the exemption.[242]

5.135 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 this exemption is one of the key outstanding issues preventing recognition of Australian privacy laws under the EU Directive, the inquiry recommended that the small business exemption be removed from the *Privacy Act*.[243]

5.136 There is support for the removal of the small business exemption[244] on the basis that: it effectively exempts 94% of all businesses from the application of the *Privacy Act*;[245] there is no reason why misuse of personal information by a small business should be treated differently from misuse by a big business;[246] consumers may not be able to determine with any certainty whether the small business exemption applies to the business they are dealing with;[247] and the removal of the small business exemption would assist to ensure that Australia's privacy law is recognised as adequate by the European Union (EU).[248] Other criticisms of the exemption include 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.[249]

5.137 One commentator has argued 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

---

241 Commonwealth, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 49 (K Curtis—Privacy Commissioner).

242 Ibid.

243 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.

244 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006; G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

245 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006.

246 G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

247 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 4; This view was supported in one submission: Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

248 M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006. Whether it is necessary or desirable for Australia's privacy law to be recognised as adequate by the EU is discussed in Ch 13.

249 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 4.

a combined turnover exceeding $3 million.[250] It was also argued that, together with the exemption for related bodies corporate,[251] the small business exemption may allow large organisations to transfer their data collection activity to a smaller entity within their corporate structure.[252]

5.138 To address the concern that the removal of the small business exemption may impact adversely on small businesses, one commentator suggested that the Privacy Commissioner should be required to make a Public Interest Determination modifying the application of the NPPs to small businesses.[253]

EU adequacy and implementation of the APEC Privacy Framework

5.139 One of the objectives of the private sector provisions was to facilitate trade with the EU.[254] In March 2001, the Article 29 Data Protection Working Party of the European Commission 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.[255]

5.140 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.[256] 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 EU adequacy. In addition, the OPC Review noted that globalisation of information makes implementation of frameworks such as the APEC Privacy Framework important. The OPC Review therefore recommended that the Australian Government continue to work with the EU on this issue, and to continue work within APEC to implement the APEC Privacy Framework.[257]

5.141 In response to questions during the 2005 Senate Committee privacy inquiry as to whether it was still necessary or desirable to achieve EU adequacy given the use of contractual privacy standards by most businesses, the Privacy Commissioner stated

---

250 Ibid, 5.

251 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.

252 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. A similar view was expressed in one submission to this Inquiry: Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

253 G Greenleaf, 'Reps Committee Protects the "Privacy-Free Zone"' (2000) 7 *Privacy Law & Policy Reporter* 1, 5.

254 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 16.

255 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.

256 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

257 Ibid, Rec 17.

that it would be simpler for businesses if they did not have to use contractual privacy provisions.[258]

5.142 According to the Australian Government Attorney-General's Department (AGD), the small business exemption appears to be the key outstanding issue cited by the EU for its conclusion that privacy protection is inadequate in Australia.[259] 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*.[260] The issue of whether it is necessary or desirable for Australia's privacy law to be recognised as adequate by the EU is discussed further in Chapter 13.

Cost of compliance

5.143 If the small business exemption was 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.

5.144 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.[261]

5.145 One commentator has 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.[262] There appears, however, to be a lack of consensus on whether the abolition of the exemption would result in high compliance costs.[263]

---

258 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.136]. The use of contractual privacy provisions to facilitate trade with EU organisations is discussed in Ch 13.

259 Ibid, [4.139].

260 Ibid, [7.33]–[7.34], Rec 12.

261 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.

262 Australian Chamber of Commerce and Industry, 'Privacy Act Review Must Not Add to Small Business Compliance Costs' (2005) 119 *ACCI Review* 1, 3.

263 One view was that there is no evidence that the abolition of the exemption would result in high compliance costs: G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006. Two stakeholders considered that if business operations were small, the cost of compliance would be low: Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006; In contrast, another stakeholder considered that the smaller the business, the heavier the regulatory burden would be on the business: A MacRae, *Consultation PC 31*, Melbourne, 5 July 2006.

Definition of 'small business'

5.146 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 [Australian Bureau of Statistics (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 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. [264]

5.147 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%.[265]

5.148 The 2000 House of Representatives Committee inquiry accepted that any form of threshold would appear arbitrary.[266] 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.[267]

5.149 Submissions to previous inquiries have consistently questioned the rationale for defining small business as businesses with an annual turnover of $3 million or less.[268] Other legislation defines small businesses differently. For example, under the uniform defamation laws, a corporation has no cause of action for defamation concerning the

---

264 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).

265 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.

266 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].

267 Ibid, [2.21].

268 Ibid, [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; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.51]–[4.52].

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.[269] The stated purpose of this provision is to prohibit corporations from suing for defamation unless they are small businesses or non-profit organisations.[270] For the purposes of the goods and services tax, small businesses are those with an annual turnover of $2 million or less.[271]

5.150 The OPC Review recommended the use of the Australian Bureau of Statistics (ABS) definition—which is currently 20 employees or fewer[272]—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.[273]

5.151 An issue raised in consultations in this Inquiry is whether it would be more appropriate to exempt businesses in terms of their turnover or the nature of information they hold, instead of the number of employees. Another issue is whether the level of the current turnover threshold of $3 million is appropriate.[274] There was also concern that stating the $3 million threshold in the *Privacy Act* makes it difficult to change.[275]

High risk sectors

5.152 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:

---

269 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).

270 See, eg, New South Wales, *Parliamentary Debates*, Legislative Assembly, 13 September 2005, 17635 (B Debus—Attorney General).

271 *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.

272 D Trewin, *Small Business in Australia—2001* (2002) Australian Bureau of Statistics.

273 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.

274 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 2006; Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

275 M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 2006.

telecommunication businesses, such as internet service providers; tenancy database operators; private detectives; debt collectors; and dating agencies.[276]

5.153 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. However, 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, then the Act does not apply.[277]

5.154 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.[278] This recommendation was rejected by the AGD because it did not believe that there was 'sufficient justification for singling out tenancy databases from the small business exemption'.[279]

5.155 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, and to those in the telecommunications sector.[280] It also recommended that the Privacy Commissioner be empowered to make a binding code under the Act to apply to all residential tenancy databases.[281] 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.[282]

5.156 In 2006, the joint working party established by the Ministerial Council on Consumer Affairs (MCCA) and SCAG 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

---

276 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].

277 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 72.

278 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.

279 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 19 June 2006.

280 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.

281 Ibid, Rec 16.

282 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.32].

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.[283] Issues concerning residential tenancy databases are discussed further in Chapter 7.

5.157 In their report, *Essentially Yours: The Protection of Human Genetic Information in Australia* (ALRC 96), the ALRC and the Australian Health Ethics Committee (AHEC) noted that there was some doubt as to whether all small businesses that hold genetic information are subject to the *Privacy Act*.[284] In their view, acts and practices of small businesses that hold genetic information pose a potential risk to the privacy of both the individual and his or her genetic relatives.[285] ALRC 96 recommended 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.[286]

5.158 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.[287] This means that small businesses that hold genetic information and provide a health service do not fall under the small business exemption.

5.159 During this Inquiry, some stakeholders have also suggested other high risk sectors to which the small business exemption should not apply, including debt collection[288] and financial services.[289]

Complexity of the exemption

5.160 In consultations, some stakeholders expressed the view that the exemption is complex and needs simplifying.[290] Based on a number of case studies, it appears that

---

283 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), 49–50.

284 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].

285 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.102].

286 Ibid, Rec 7–7.

287 *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).

288 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

289 Ibid; D Mico, *Consultation PC 9*, Sydney, 14 March 2006.

many small businesses do not understand the operation of the *Privacy Act*.[291] A view was also expressed that there is some misunderstanding among small businesses as to whether or not they are exempt.[292]

Consent provisions

5.161 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.[293] 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.[294] 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.[295]

Voluntary compliance and opting in

5.162 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.[296] 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.[297]

---

290 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

291 M Jackson and others, *Small Business: Issues of Identity Management, Privacy and Security* (2006), 10.

292 A MacRae, *Consultation PC 31*, Melbourne, 5 July 2006.

293 *Privacy Act 1988* (Cth) s 6D(7), (8).

294 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.

295 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/tel/numbering> at 12 September 2006. 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.

296 M Jackson and others, *Small Business: Issues of Identity Management, Privacy and Security* (2006), 9–10.

297 Ibid, 9–10.

Question 5–6 Should the small business exemption remain? If so: (a) what should be its extent; and (b) should an opt-in procedure continue to be available?

Registered political parties, and political acts and practices

5.163 A 'registered political party' is specifically excluded from the definition of 'organisation' and is therefore exempt from the operation of the *Privacy Act*.[298] In addition, political acts and practices of certain organisations are also exempt.[299] 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.[300] Acts and practices covered by the exemption include elections held under an electoral law;[301] 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.[302]

5.164 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. The persons and entities that are entitled to this information include candidates for an election, registered political parties, Members of Parliament, and state and territory electoral authorities.

5.165 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 the Members of Parliament of their functions as parliamentarians concerning enrolled persons.[303] Section 91B of the *Commonwealth Electoral Act* makes it an offence to use the information obtained under the Act for commercial purposes.

5.166 In his second reading speech on the Privacy Amendment (Private Sector) Bill, 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

298 *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).
299 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7C.
300 Ibid s 7C.
301 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).
302 Ibid s 7C.
303 *Commonwealth Electoral Act 1918* (Cth) s 91A.

> operation of the electoral and political process in Australia. I am confident that it will not unduly impede the effective operation of the legislation.[304]

5.167 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.[305] In his view:

> 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 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.[306]

5.168 In June 2006, Senator Natasha Stott Despoja introduced a Private Member's Bill to remove the exemption for political acts and practices.[307] 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.[308]

5.169 For the period from 21 December 2001 to 31 January 2005, the OPC stated that 0.4% of all the NPP complaints closed by the Office as outside of its jurisdiction concerned the political exemption.[309]

Electoral databases

5.170 Electoral databases are databases maintained by political parties that contain information on voters, which may include voters' policy preferences and party identification.[310] 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

---

304 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General), 15753.

305 M Crompton (Federal Privacy Commissioner), 'Media Release: Federal Privacy Commissioner, Malcolm Crompton Comments on Private Sector' (Press Release, 12 April 2000).

306 Ibid.

307 Privacy (Extension to Political Acts and Practices) Amendment Bill 2006 (Cth). At the time of writing, the Bill has been read for the first time in the Senate.

308 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 10.

309 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

310 P van Onselen and W Errington, 'Electoral Databases: Big Brother or Democracy Unbound?' (2004) 29 *Australian Journal of Political Science* 349, 349.

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.[311]

5.171 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.[312]

5.172 Proposals for reform in this area include: allowing FOI 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 and supporting 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 of the database software; and transferring voter information to a central database to which all politicians have access.[313]

International instruments

5.173 The Explanatory Memorandum to the OECD Guidelines states that exceptions to the privacy principles are to be limited to those that are 'necessary in a democratic society'.[314] The 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.[315] Under the Directive, the processing of data by political organisations for marketing purposes is also permitted subject to certain conditions.[316] The APEC Privacy Framework does not contain a specific exemption or exception concerning political or electoral activities.

5.174 In September 2005, an international conference of privacy and data protection commissioners, including the federal Privacy Commissioner, adopted a *Resolution on the Use of Personal Data for Political Communication*.[317] The Resolution states that

---

311 P van Onselen and W Errington, 'Suiting Themselves: Major Parties, Electoral Databases and Privacy' (2005) 20 *Australasian Parliamentary Review* 21, 28.

312 P van Onselen and W Errington, 'Electoral Databases: Big Brother or Democracy Unbound?' (2004) 29 *Australian Journal of Political Science* 349, 362–363.

313 P van Onselen and W Errington, 'Political Party Databases: Proposals for Reform' (2004) 6 *Australian Journal of Professional and Applied Ethics* 82.

314 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Explanatory Memorandum, [47].

315 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.

316 Ibid, Recital 30.

317 *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 30 August 2006.

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.[318]

Issues and problems

Removal or modification of the exemption

5.175 In its review of the Privacy Amendment (Private Sector) Bill, the 2000 House of Representatives Committee inquiry noted that the 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 inquiry's view, for parliamentarians properly to represent their constituents, they must respond in a more targeted way to their electorate, which requires that they collect and use certain information concerning constituents.[319]

5.176 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.[320] 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'.[321] The AGD rejected the recommendation on the basis that this would narrow significantly the scope of the exemption.[322]

5.177 The 2000 House of Representatives Committee inquiry also recommended that a new provision be inserted to provide that the exemption did not allow political parties or political representatives to sell or disclose personal information collected in the course of their duties to anyone not covered by the exemption.[323] The AGD rejected this recommendation, on the basis that the exemption would operate in a manner that would address the inquiry's concern.[324] However, a note was inserted in the Bill to

---

318 Ibid. Data protection principles are discussed in Ch 4.

319 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].

320 Ibid, [5.46].

321 Ibid, Recs 11, 12.

322 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 19 June 2006.

323 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.

324 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 19 June 2006.

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.[325]

5.178 A number of submissions to the 2005 Senate Committee privacy inquiry strongly objected to the exemption for political acts and practices.[326] The OPC stated that it had received relatively few complaints and inquiries about the exemption.[327] The 2005 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.[328]

Implied freedom of political communication

5.179 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.[329] The High Court has established that an essential element of representative democracy is the freedom of public discussion of political and economic matters.[330] This freedom is not confined to election periods.[331] It does not, however, confer a personal right on individuals, but rather operates as a restriction on legislative and executive powers.[332] The freedom is not absolute,[333] 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 …[334]

---

325 Further Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [1]; *Privacy Act 1988* (Cth), note to s 7C.

326 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.87]–[4.94].

327 Ibid, [4.95]–[4.96].

328 Ibid, [7.29]–[7.30], Rec 11.

329 *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.

330 *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.

331 *Cunliffe v Commonwealth* (1994) 182 CLR 272, 327; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 560–561.

332 *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104, 168; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 561.

333 *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.

334 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567.

5.180 One option for ensuring that coverage of political acts and practices by the *Privacy Act* did not contravene the implied freedom of political communication would be to provide that the *Privacy Act* 'does not apply to the extent … that it would infringe any constitutional doctrine of implied freedom of political communication'.[335]

Question 5–7 Should registered political parties be exempt from the operation of the privacy principles in the *Privacy Act*?

Question 5–8 Should political acts and practices be exempt from the operation of the *Privacy Act*? If so, does the current exemption under s 7C of the *Privacy Act* strike an appropriate balance between the protection of personal information and the implied freedom of political communication?

Employee records exemption

5.181 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.[336]

335 Australian Government Office of Parliamentary Counsel, *Drafting Direction No 3.1—Constitutional Law Issues* (2006), [8].

336 *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.

5.182 Acts and practices of a current or former employer in relation to an employee record are exempt from the *Privacy Act* if they are directly related to the current or former employment relationship.[337] Accordingly, the exemption does not apply to: acts and practices of an employer that are beyond the scope of the employment relationship;[338] the personal information of unsuccessful job applicants;[339] and the handling of employee records by contractors and subcontractors to the employer.[340] The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 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.[341]

5.183 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.[342]

5.184 The AGD stated 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.[343]

5.185 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. However, this only applies to records about conditions under which employees are hired, hours

---

337 *Privacy Act 1988* (Cth) ss 7(1)(ee), 7B(3).

338 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.

339 However, once an employment relationship is established, 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.

340 Ibid, 4. The OPC 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.

341 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [109].

342 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].

343 Australian Government Attorney-General's Department, *Fact Sheet on Privacy in the Private Sector—Employee Records* (2000) <www.ag.gov.au> at 19 June 2006.

worked, remuneration, leave, superannuation contributions and termination.[344] 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.

5.186 There is no corresponding exemption for the handling of employee records by public sector agencies under the *Privacy Act*. Therefore, Australian Government and ACT public sector agencies are required to comply with the IPPs when dealing with employee records.[345] Privacy legislation in New South Wales, Victoria and the Northern Territory also extends to employee records of public sector employees.[346] 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.[347] 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.

5.187 In February 2004, the AGD and the Department of Employment and Workplace Relations (DEWR) released a discussion paper on the privacy of employee records.[348] 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.[349]

5.188 In April 2006, SCAG agreed to establish a working group to advise ministers on options for improving consistency in privacy regulation, including workplace privacy.[350] In its response to the 2006 report by the Productivity Commission's

---

344 *Workplace Relations Regulations 2006* (Cth) regs 19.7–19.16.

345 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.

346 *Privacy and Personal Information Protection Act 1998* (NSW); *Information Privacy Act 2000* (Vic); *Information Act 2002* (NT).

347 *Personal Information Protection Act 2004* (Tas) ss 3 (definition of 'personal information custodian'), 10, sch 1 cl 2(1)(i)–(j).

348 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).

349 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].

350 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.

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.[351]

5.189 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. However, they commonly provide for exceptions to their data protection principles when dealing with personal information for the purposes of recruitment, appointments and contracts for provision of services.[352] Some overseas legislation also provides an exception for personal references relevant to an individual's suitability for employment or appointment to office.[353]

5.190 There is no general exemption for employee records under the OECD Guidelines, the EU Directive or the APEC Privacy Framework.[354] In 2001, the Article 29 Data Protection Working Party of the European Commission released its advisory opinion on the *Privacy Amendment (Private Sector) Act*. 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 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.[355]

5.191 For the period from 21 December 2001 to 31 January 2005, the OPC indicated that 12% of all the NPP complaints closed by the Office as outside of its jurisdiction concerned the employee records exemption.[356] In 2004–05, the OPC received 2,469

---

351 Ibid, 26.

352 See, eg, *Data Protection Act 1998* (UK) sch 7 cls 3, 4; *Data Protection Act 1988* (Ireland) s 4(13); *Privacy Act 1993* (NZ) s 29; *Personal Data (Privacy) Ordinance* (Hong Kong) s 55.

353 See, eg, *Data Protection Act 1998* (UK) sch 7 cl 1; *Data Protection Act 1988* (Ireland) s 4(13)(b); *Privacy Act 1993* (NZ) s 29(1)(b); *Personal Data (Privacy) Ordinance* (Hong Kong) s 56.

354 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].

355 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.

356 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

enquiries concerning exemptions, of which 48% related to the employee records exemption.[357]

Issues and problems

Adequacy of privacy protection for employee records

5.192 In its inquiry into the Privacy Amendment (Private Sector) Bill, the 2000 House of Representatives Committee stated that it 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.[358]

5.193 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. In the inquiry's view, employees are entitled to expect confidentiality of their workplace records given that they have little choice about providing information to their employers.[359]

5.194 In rejecting the recommendations by the 2000 House of Representatives Committee inquiry, the AGD 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 (Private Sector)] Bill might result in an unacceptable level of interference with those State and Territory laws, and a confusing mosaic of obligations.[360]

---

357 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 38.

358 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].

359 Ibid, [3.30]–[3.33].

360 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 19 June 2006. 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.

5.195 The 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 best protect employee records.[361]

5.196 In its report, *Workplace Privacy*, the Victorian Law Reform Commission commented that 'the operation of the employee records exemption leaves a significant gap in the privacy protection of workers' personal information'.[362]

5.197 In consultations, many stakeholders expressed concern about the employee records exemption.[363] Several stakeholders expressed the view that employee records should be within the scope of the *Privacy Act*[364] on the basis that: intrusion into employees' privacy has great potential to cause harm to individuals;[365] and employee records are a major area of information held by organisations.[366]

Scope of the exemption

5.198 The 2000 House of Representatives Committee inquiry acknowledged that there is a difference between 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.[367]

5.199 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. It recommended that the other matters listed in the proposed definition of 'employee record' be subject to the NPPs.[368] The inquiry was also of the view that employees' personal information is sensitive regardless of the size of the employer and therefore the recommendations also should apply to small business employers.[369] The

---

361 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.

362 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [1.19].

363 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006; G Hill, *Consultation PC 21*, Melbourne, 8 May 2006; Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

364 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006; I Cunliffe, *Consultation PC 23*, Melbourne, 9 May 2006; G Hill, *Consultation PC 21*, Melbourne, 8 May 2006.

365 N Waters, *Consultation PC 17*, Sydney, 2 May 2006.

366 Public Interest Advocacy Centre, *Consultation PC 29*, Sydney, 16 May 2006.

367 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].

368 Ibid, Recs 5–7.

369 Ibid, [3.40].

recommendations were not intended to override the provisions in the workplace relations legislation.[370] The inquiry's recommendations were rejected by the AGD.[371]

5.200 A number of stakeholders have expressed the view that any changes to the scope of the employee records exemption should allow for free and frank discussion between referees and prospective employers.[372]

5.201 Another issue concerns 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.[373]

5.202 In ALRC 96, the ALRC and AHEC recommended that the *Privacy Act* be extended to cover genetic information contained in employee records.[374] They further recommended that the inter-departmental review of employee privacy by the AGD and DEWR consider whether the *Privacy Act* should be amended to cover other forms of health information contained in employee records.[375]

EU adequacy and implementation of the APEC Privacy Framework

5.203 The EU has not granted Australia 'adequacy status' under the EU Directive. The 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.[376] It recommended that the Australian Government continue to work with the EU on this issue and continue to work within APEC to implement the APEC Privacy Framework.[377]

5.204 In response to questions during the 2005 Senate Committee privacy inquiry, the AGD noted that negotiations with the EU were continuing, and that the prospects for

---

370 Ibid, [3.39].

371 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 19 June 2006.

372 M Hunter, *Submission PR 16,* 1 June 2006; M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 2006; D Mico, *Consultation PC 9*, Sydney, 14 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

373 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.37].

374 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.

375 Ibid, Rec 34–2.

376 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

377 Ibid, Rec 17.

resolving the situation were good in the medium term.[378] The issue of EU adequacy is discussed further in Chapter 13.

Location of privacy provisions concerning employee records

5.205 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 was 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 contribute to problems of inconsistency and fragmentation. It therefore recommended that the privacy of employee records be protected under the *Privacy Act*.[379]

5.206 In its submission to the review of employee records privacy by the AGD and DEWR, the ALRC stated that the existence of the employee records exemption only increases the level of complexity of the *Privacy Act*, and that 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.[380]

Question 5–9 Should the employee records exemption remain? If so: (a) what should be the scope of the exemption; and (b) should it be located in the *Privacy Act*, workplace relations legislation or elsewhere?

Media exemption

5.207 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 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 that collects, prepares or disseminates to the public, news, current affairs, information or documentaries; or commentaries and opinions on, or analyses of, such material.[381]

5.208 The phrase 'in the course of journalism' has not been defined or judicially considered in Australia. When the Privacy Amendment (Private Sector) Bill was first introduced, 'journalism' was defined as the collection, preparation and dissemination

---

378 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.138].

379 Ibid, [7.36]–[7.37], Rec 13.

380 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.

381 *Privacy Act 1988* (Cth) s 6(1).

of news, current affairs, documentaries and other information to the public.[382] However, the definition was omitted from the Act 'so that the ordinary meaning of the word will apply'.[383] 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.[384] The terms 'news', current affairs' and 'documentary' are also not defined.

5.209 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.[385]

5.210 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 adequately safeguarding the handling of information.[386]

5.211 The broadcast media is regulated by the *Broadcasting Services Act*. The Act requires radio and television industry groups to develop, in consultation with ACMA, codes of practice to apply to the broadcasting operations of each section of the broadcasting industry.[387] Industry codes that have been approved by ACMA are included on ACMA's Register of Codes of Practice.[388] ACMA may impose a licence condition requiring the broadcasting licensees to comply with an applicable code of practice.[389] Section 139 of the *Broadcasting Services Act* makes it 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.[390]

---

382 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13.

383 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [2].

384 Supplementary Explanatory Memorandum, Privacy Amendment Bill 1989 (Cth), [4].

385 See also *Uniform Evidence Law*, where the ALRC recommended that the uniform Evidence Acts be amended to provide for a professional confidential relationship privilege, including the privilege between journalists and their sources. It recommended that the privilege apply to any compulsory process for disclosure, such as pre-trial discovery and the production of documents in response to a subpoena, and in non-curial contexts as well as court proceedings: 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.

386 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 United Nations' *International Covenant on Civil and Political Rights 1966.* Article 19 of the Covenant provides in part that everyone shall have the right to freedom of expression, including the freedom to seek, receive and impart information and ideas. The exercise of the right may, however, be subject to certain restrictions: *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).

387 *Broadcasting Services Act 1992* (Cth) s 123.

388 Ibid s 123(4).

389 Ibid ss 44(2), 88(2), 92J(2), 100(2), 119(2).

390 Ibid s 125.

5.212 ACMA has also developed *Privacy Guidelines for Broadcasters*, which 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.[391]

5.213 The Australian Press Council (APC) is a self-regulatory body that deals with the print media. It aims to help preserve the freedom of the press within Australia and ensure that the press acts responsibly and ethically.[392]

5.214 The APC has published a set of *Privacy Standards* for the purposes of the media exemption under the *Privacy Act*. The APC receives and deals with complaints about possible breaches of these Standards,[393] 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.[394] The APC secretariat will try to negotiate the settlement of a complaint, failing which a formal response will be sought from the newspaper and sent to the complainant. If the complainant is not satisfied by the response, he or she can, with the agreement of the newspaper, seek a conciliation hearing conducted by a public member of 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.[395]

5.215 The Media Entertainment and Arts Alliance is the union and professional organisation for the media, entertainment, sports and arts industries.[396] Journalist members of the Alliance are bound by the Alliance's *Code of Ethics*. The *Code of Ethics* provides for certain privacy standards, including the requirements 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.[397]

5.216 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.

---

391 Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), 1.

392 Australian Press Council, *About the Council* <www.presscouncil.org.au/pcsite/apc.html> at 5 September 2006.

393 Australian Press Council, *Privacy Standards* <www.presscouncil.org.au> at 16 June 2006.

394 Australian Press Council, *How to make a Complaint: An Overview* <www.presscouncil.org.au/pcsite/complain.html> at 5 September 2006.

395 Ibid.

396 Alliance Online, *Alliance* <www.alliance.org.au> at 6 September 2006.

397 Media Entertainment and Arts Alliance, *Code of Ethics* <www.alliance.org.au> at 6 September 2006, [2], [8], [11].

Information about complaints against journalists is published and distributed on an annual basis to journalist members of the Alliance.[398] The Alliance has no powers to act against or sanction a journalist who is not one of its members.

5.217 The OPC Review noted that the OPC had received very few inquiries and complaints about media organisations.[399] 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.[400]

5.218 A number of overseas jurisdictions provide for an exemption relating to journalistic materials or news activities, including the United Kingdom, New Zealand and Canada.[401] The United Kingdom and Canadian data protection legislation provides that personal information collected for journalistic, artistic or literary purposes is exempt. The New Zealand *Privacy Act 1993* provides that the term 'agency' does not include news media in relation to their news activities.[402] In Hong Kong, instead of a general exemption for the media, news activities are treated as an exception to some of the data protection principles.[403]

Issues and problems

Scope of the exemption

5.219 One issue raised is whether the media exemption strikes 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.[404] Several stakeholders

---

398 Alliance Online, *Code of Ethics Breaches: How to Complain* <www.alliance.org.au/media/ethics_breach.htm> at 6 September 2006.

399 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 197. However, the Australian Privacy Foundation submitted 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': Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

400 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 328.

401 *Data Protection Act 1998* (UK) s 32; *Privacy Act 1993* (NZ) s 2(1); *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) s 7(1)(c).

402 *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).

403 *Personal Data (Privacy) Ordinance* (Hong Kong) s 61.

404 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 as well as consultations in this Inquiry: Office of the Privacy

have expressed the view that the media exemption requires reconsideration.[405] The APC 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.[406]

5.220 In its 1979 report *Unfair Publication* (ALRC 11), a majority of the ALRC recommended that 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. Sensitive private facts are matters relating to the health, private behaviour, home life, or personal or family relationships of an individual.[407] The recommendation has not been implemented.

5.221 Concerns have also been raised that media reporting of health information runs a high risk of causing harm to individuals and therefore should be subject to tighter regulation.[408]

Definitions

5.222 Originally, the term 'journalism' was defined in the Privacy Amendment (Private Sector) Bill. After the release of the 2000 House of Representatives Committee inquiry report, the Australian Government amended the Bill to omit the definition of 'journalism'.[409] In response to questions by the 2000 Senate Committee inquiry, the 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.[410]

5.223 In its review of the private sector provisions of the *Privacy Act*, the OPC recommended the term 'in the course of journalism' be defined and that the term

---

Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 196–197; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

405 M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006; M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 2006; Commonwealth Ombudsman, *Consultation PC 11*, Canberra, 30 March 2006; A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006; D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

406 Australian Press Council, *Submission PR 48,* 8 August 2006.

407 Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [236].

408 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.

409 Supplementary Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), [2]–[4].

410 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Provisions of the Privacy Amendment (Private Sector) Bill 2000* (2000), [3.29].

'media organisation' be clarified in order to ensure that the exemption focuses on news and current affairs.[411]

5.224 It has been argued that due to the lack of 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,[412] including any organisation that collects and disseminates personal information over the internet.[413]

Adequacy of the self-regulatory model

5.225 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.[414] 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.[415]

5.226 In response to these recommendations the AGD stated that it was not appropriate to require independently operating journalists and media organisations to subscribe to a model media code developed by the Privacy Commissioner before allowing them the benefit of the exemption.[416]

5.227 One commentator argues that the current self-regulatory model should remain.[417] In his view, the only practical alternative is a government-appointed body,

---

411 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.

412 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.

413 M Neilsen, *Privacy Amendment (Private Sector) Bill 2000: Bills Digest No 193 1999–2000* (2000) Parliament of Australia—Parliamentary Library, 13.

414 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].

415 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.

416 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 19 June 2006.

417 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.

but that would be undesirable because the right to publish freely without fear of government intervention is fundamental to a democratic society.[418]

5.228 In its 2004 report on privacy and media intrusion, the Law Reform Commission of Hong Kong recommended a co-regulatory approach and the establishment of an independent and self-regulating statutory commission to deal with privacy complaints against the print media.[419]

Criteria for media privacy standards

5.229 The *Privacy Act* has been criticised for its lack of criteria for, or independent assessment of, the adequacy of media privacy standards.[420] The adequacy of the media privacy standards has also been questioned.[421] 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.[422]

5.230 The OPC Review also recommended that the Australian Government consider amending the *Privacy Act* so that the Australian Broadcasting Authority (now ACMA) be required to consult with the Privacy Commissioner when developing privacy codes.[423] The OPC Review further recommended that the OPC, together with the Australian Broadcasting Authority, provide 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.[424]

Enforcement mechanisms

5.231 Concerns have been raised about the lack of adequate enforcement mechanisms for the media privacy standards. For example, in its submission to the OPC Review,

---

418 D Pearce, 'Privacy and the Press: Issues of Balance and Perspective' (2003) 10 *Privacy Law & Policy Reporter* 132, 138.

419 Law Reform Commission of Hong Kong, *Privacy and Media Intrusion* (2004), Rec 5.

420 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.

421 D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

422 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 198.

423 Ibid, Rec 58.

424 Ibid, Rec 59.

the Australian Broadcasting Authority submitted that there are no appropriate sanctions that would allow it actively to enforce the privacy provisions in codes of practice for the broadcasting media.[425]

5.232 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.[426] In addition, it has been argued that the 'penalty' imposed by the APC is not a deterrent.[427]

Question 5–10 Should acts and practices of media organisations in the course of journalism be exempt from the operation of the *Privacy Act*? If so: (a) what should be the scope of the exemption; and (b) does s 7B(4) of the *Privacy Act* strike an appropriate balance between the free flow of information to the public and the protection of personal information?

Question 5–11 Should the terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' be defined in the *Privacy Act*? If so, how should they be defined? Are there other terms that would be more appropriate?

Question 5–12 If the media exemption is retained, how should journalistic acts and practices be regulated?

Personal or non-business use

5.233 Individuals are included in the definition of an 'organisation' in the *Privacy Act*.[428] 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 NPPs do not apply where information is dealt with solely in the context of an individual's personal, family or household affairs.

5.234 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 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.[429] 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, family

425 Australian Broadcasting Authority, *Submission to Review of the Private Sector Provisions of the Privacy Act 1988*, 1 December 2004.
426 N Waters, 'Can the Media and Privacy Ever Get On?' (2002) 9 *Privacy Law & Policy Reporter* 149.
427 Ibid.
428 *Privacy Act 1988* (Cth) s 6C(1)(a).
429 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [106].

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'.[430]

5.235 Both the EU Directive and the APEC Privacy Framework provide that they do not apply to the handling of personal information in connection with an individual's personal, family or household affairs.[431] This exemption is commonly provided for in overseas jurisdictions, for example, the United Kingdom, New Zealand, Canada and Hong Kong.[432]

5.236 In its submissions to the OPC Review and the 2005 Senate Committee privacy inquiry, 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'.[433] In submissions and consultations in this Inquiry, similar concerns have been raised in relation to the posting of photographs and offensive comments on websites and 'blogs'.[434] These issues are discussed further in Chapter 11.

Related bodies corporate

5.237 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.[435] The exemption does not extend to 'sensitive information',[436] which is defined to include health information and personal information such as an

430 Ibid, notes on clauses [164].

431 Article 3(2) of the EU Directive provides that the Directive 'shall not apply to the processing of personal data: … by a natural person in the course of a purely personal or household activity': 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. Under paragraph 10 of the APEC Privacy Framework, the definition of 'personal information controller' excludes an individual who handles personal information in connection with the individual's personal, family or household affairs: Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [10].

432 *Data Protection Act 1998* (UK) s 36; *Privacy Act 1993* (NZ) s 56; *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) s 4; *Personal Data (Privacy) Ordinance* (Hong Kong) s 52.

433 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.

434 Confidential, *Submission PR 49,* 14 August 2006; M Paterson, *Consultation PC 26*, Melbourne, 9 May 2006; M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 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 University, *The Macquarie Dictionary (online edition)*, Macquarie Library Pty Ltd, 15 August 2006.

435 *Privacy Act 1988* (Cth) s 13B(1).

436 Ibid s 13B(1).

individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, sexual preferences and criminal record.[437]

5.238 A 'related body corporate' is defined in s 50 of the *Corporations Act 2001* (Cth) 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.[438]

5.239 In addition, although related companies may share personal information, the handling of that information is still subject to the NPPs.[439] For example, each company within the group of related companies in other respects must use the information consistently with the primary purpose for which it was originally collected, and may only use the personal information for a secondary purpose where that purpose is allowed by NPP 2.1.[440]

5.240 The exemption does not apply if the company is a contractor under a Commonwealth contract and: (a) the collection from or disclosure of personal information to the related company is contrary to a contractual provision; or (b) the collection of personal information is for the purpose of meeting an obligation under the contract and the disclosure is for direct marketing purposes.[441]

5.241 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; 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.[442] The stated reason for this exemption is to 'recognise

437 Ibid s 6(1).
438 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [139].
439 *Privacy Act 1988* (Cth), note to s 13B(1); Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [141].
440 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [141].
441 *Privacy Act 1988* (Cth) s 13B(2).
442 Ibid s 13E.

[the] commercial reality that, for many bodies corporate to continue to operate effectively, they need to be able to communicate with related bodies corporate'.[443]

5.242 The 2000 House of Representatives Committee inquiry accepted that it is not realistic to ignore the fact that many businesses are structured in a way that uses more than one legal entity. The inquiry 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.[444] 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 that will be shared within the members of that group.[445]

5.243 This exemption has been criticised as a potential loophole through which corporate groups could evade the coverage of the *Privacy Act*.[446] In its submissions to the OPC Review and the 2005 Senate Committee privacy inquiry, Electronic Frontiers Australia Inc. (EFA) submitted that the exemption enables large businesses intentionally to structure their affairs to take advantage of the 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. The EFA submitted that the exemption should be removed and that related bodies corporate should be treated as third parties.[447]

5.244 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 13.

Change in partnership

5.245 In certain circumstances an act or practice is not an interference with the privacy of an individual if it consists of the passing of personal information from an old to a new partnership.[448] The new partnership must: be forming at the same time or immediately after the old one; have at least one partner transferred from the old

443 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [138].

444 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].

445 Ibid, Rec 21.

446 Ibid, [9.9].

447 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.

448 *Privacy Act 1988* (Cth) s 13C.

partnership; and carry on the same or a similar business as the old partnership.[449] 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.[450]

5.246 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; 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.[451]

Required by foreign law

5.247 Acts and practices that occur outside Australia and the external territories that are required by an applicable foreign law are not interferences with the privacy of an individual or a breach of the NPPs (or an approved privacy code).[452] However, such overseas acts and practices may be interferences with privacy if they: 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; 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.[453]

5.248 The stated purpose of this exemption is 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'.[454]

Question 5–13 Do any issues arise concerning related bodies corporate, changes in partnership and overseas acts required by foreign law in Part III Division 1 of the *Privacy Act*? If so, how should they be dealt with?

New exemptions?

5.249 This section considers new exemptions that have been suggested for inclusion in the *Privacy Act*.

449 Ibid s 13C(1).
450 Ibid, note to s 13C(1).
451 Ibid s 13E.
452 Ibid ss 6A(4), 6B(4), 13D(1).
453 Ibid s 13E.
454 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), notes on clauses [65], [70].

Valuers

5.250 Valuers assess the value of a wide range 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.[455]

5.251 In a joint submission to the Privacy Commissioner, the Australian Property Institute and the Real Estate Institute of Australia (REIA) raised concerns about difficulties in determining the impact of privacy laws on the property sector.[456] In response to the joint submission, the Privacy Commissioner stated that 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—would be disclosed for valuation purposes. However, individual vendors or purchasers would not reasonably expect a real estate agent to disclose their names to valuers. In the Privacy Commissioner's view, valuation work can proceed without significant impedient by ensuring that individuals are aware that their sales-related information may be used or disclosed for valuation purposes. This may require real estate agents, valuers and their peak bodies to take steps to raise the awareness of the community about such use and disclosure.[457]

5.252 In its submission to this Inquiry, the 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 as a result of the *Privacy Act*, the ability of valuers to collect up-to-date and reliable personal and property information have been diminished.[458]

Professional archivists and archival organisations

5.253 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.

5.254 In a submission to the AGD on the Privacy Amendment (Private Sector) Bill, the Australian Society of Archivists Inc and the Australian Council of Archives

---

455 *Valuers Regulation 2005* (NSW) reg 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.

456 'Privacy Legislation and It's Effect on the Valuation Industry' (2003) *Australian Property Journal* 517, 517.

457 Ibid, 518.

458 Real Estate Institute of Australia, *Submission PR 7,* 10 April 2006.

proposed an exemption of archival institutions from the operation of the NPPs to allow the possibility of continued research into the administrative, corporate, cultural and intellectual activity of Australia—in particular, social and genealogical research.[459] The issue of whether privacy principles should cover social research is discussed in Chapter 4.

5.255 The ALRC is interested in hearing whether there are entities or types of activities that should be exempt from the operation of the *Privacy Act*.

Question 5–14 Are there any other entities or types of activities that should be exempt from the operation of the *Privacy Act*? If so, what are those entities or types of activities, and what should be the scope of the exemption?

459 Australian Society of Archivists Inc, *Submission to the Federal Privacy Commissioner on the Draft National Privacy Principle Guidelines* (2001) <www.archivists.org.au/council/subs/privacyprinciples.html> at 23 June 2006.

6. Powers of the Office of the Privacy Commissioner

Contents

Introduction

6.1 This chapter discusses two key elements in effective privacy protection. The first element is the Office of the Privacy Commissioner (OPC), the statutory body established by the *Privacy Act 1988* (Cth) to oversee and enforce the *Privacy Act.* The second element concerns the procedures established by the *Privacy Act* for monitoring and securing compliance with the Act. This chapter considers both of these elements and raises issues about the effectiveness of the current statutory provisions in ensuring agencies and organisations comply.

Office of the Privacy Commissioner

Arrangement

6.2 The OPC is established by s 19 of the *Privacy Act* and consists of the Privacy Commissioner (Commissioner), the staff necessary to assist the Commissioner, and consultants the Commissioner engages.[1] The Commissioner convenes and receives the assistance of the Privacy Advisory Committee (described below).[2]

6.3 The Commissioner is appointed by the Governor-General for a period not exceeding seven years.[3] The *Privacy Act* imposes conditions on the Commissioner's appointment, and the Governor-General may determine that other conditions also apply.[4] The Governor-General 'may' terminate the Commissioner's appointment by reason of misbehaviour or incapacity[5] and 'shall' terminate in other specified circumstances (such as bankruptcy).[6]

---

1 *Privacy Act 1988* (Cth) ss 19, 19A(1), 26A(1), 26A(3).
2 Ibid s 82.
3 Ibid ss 19A(1), 20(1).
4 Ibid s 20.
5 Ibid s 25(1).
6 Ibid s 25(2). This is in contrast to the recommendations of the Victorian Law Reform Commission which recommends that a proposed regulator of workplace privacy legislation should only be removable from office if he or she commits a criminal offence or becomes incapable because of physical or mental incapacity: Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.14], Rec 34.

Role of the OPC

General description

6.4 The OPC describes its role as follows:

> The Office plays an active role in raising awareness about individuals' privacy rights and in addressing their concerns about possible interference with their rights. It provides information by way of its information hotline and its web site. The web site contains all the Office's publications, answers to Frequently Asked Questions, media comments, media releases, speeches, case notes, an online complaint checker, multi-lingual web pages, guidelines, information sheets, brochures and the annual report.
>
> To the extent that the Office's activities in raising awareness are successful, community confidence that individuals' rights are protected is likely to be increased. If an individual's privacy rights are interfered with and he or she cannot resolve the issue with the organisation concerned, the Office will investigate the complaint, conciliate it, if appropriate, or make a determination.[7]

6.5 To enable the OPC to perform this role, the *Privacy Act* vests in the Commissioner numerous liberties, privileges, functions, powers, immunities and obligations.

Functions and powers

6.6 The general approach of the *Privacy Act* is to state the Commissioner's 'functions' (found principally in ss 27–29 of the Act) 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'.[8]

6.7 The Commissioner's functions and powers are considered in three groups: oversight powers; compliance powers, including powers to monitor compliance and to investigate and resolve complaints; and powers in relation to privacy codes.

6.8 Before discussing each group of powers, two provisions should be noted immediately. First, the Commissioner 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).[9] The express functions and powers of the Commissioner therefore do not need to be construed narrowly.

6.9 Secondly, the Commissioner has a power of delegation. The Commissioner may delegate the exercise of all or any of his or her powers either to a member of the

---

7 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 105.

8 *Privacy Act 1988* (Cth) ss 27(2), 28(2), 28A(2).

9 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).

Commissioner's staff or a member of the staff of the Ombudsman.[10] However, powers conferred by s 52—'Determination of the Commissioner'—and powers in connection with the performance of the function of the Commissioner set out in s 28(1)(a)—which concerns tax file numbers—are non-delegable.

Manner of exercise

6.10 The *Privacy Act* regulates in two ways the manner in which the Commissioner's powers may be exercised. 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;[11] 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.[12]

6.11 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, within the limitations of Commonwealth power,[13] and are consistent with whichever of the Information Privacy Principles (IPPs), the National Privacy Principles (NPPs) and the Code of Conduct (relating to credit reporting) and Part IIIA (Credit reporting), if any, is relevant.[14]

Liabilities and immunities

6.12 The *Privacy Act* confers a number of liabilities and immunities on the Commissioner and other persons.

Liabilities

6.13 Decisions of the Commissioner are subject to judicial review if they are not made properly within the framework set out above. More generally, as an administrative officer of the Commonwealth, the Commissioner is subject to the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (the ADJR Act), and the

---

10 *Privacy Act 1988* (Cth) s 99.

11 Ibid s 29(a). 'The legislation recognises 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': Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 28.

12 *Privacy Act 1988* (Cth) s 29(b).

13 Ibid s 29(c).

14 Ibid s 29(d).

administrative law doctrines of excess and abuse of power. Matters that could be the subject of an application for review under the ADJR Act include a decision that a privacy complaint will not be investigated, a decision not to make a determination, and a failure to give reasons to a person adversely affected by a decision of the Commissioner.[15] Further, the Commissioner (and thereby the OPC) is subject to the Commonwealth Ombudsman's powers with respect to 'a matter of administration'.[16]

6.14 The Commissioner and his or her staff and delegates are subject to criminal liability in some circumstances. It is an offence for a person who is or has been the Commissioner, or a member of the Commissioner's staff, or who has at any time acted for or on behalf of the Commissioner, to disclose, use or make a record of information acquired about another person in performance of that role—other than to do something permitted or required by the *Privacy Act*.[17] A kind of privilege regarding such information is also created: such a person is not obliged to divulge or communicate that information except as required or permitted by the *Privacy Act*.[18]

Immunities

6.15 The Commissioner enjoys partial immunity from civil actions. He or she is not 'liable to an action, suit or proceeding in relation to an act done or omitted to be done in good faith in the exercise or purported exercise of any power or authority conferred by [the *Privacy Act*]'.[19] This immunity also applies to an adjudicator for an approved privacy code, as well as delegates of the Commissioner or adjudicator.[20]

6.16 The *Privacy Act* also furnishes some legal protection to other persons. In particular, civil proceedings will not lie against a person in respect of loss, damage or injury suffered by that person because of certain acts done in good faith—the making of a complaint under the *Privacy Act* or approved privacy code, the acceptance by the Commissioner of a complaint referred by an adjudicator, or the making of a statement or giving of a document or information to the Commissioner.[21]

---

15 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.

16 *Ombudsman Act 1976* (Cth) s 15(1); Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 128.

17 *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).

18 *Privacy Act 1988* (Cth) s 96(2), (4).

19 Ibid s 64(1).

20 Ibid s 64.

21 Ibid s 67.

6.17 Further, 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.[22]

Privacy Advisory Committee

6.18 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.[23] The functions of the Advisory Committee include advising the Commissioner on matters relevant to the Commissioner's functions, either on its own initiative or at the Commissioner's request, recommending material to be included in guidelines issued by the Commissioner, and, subject to any directions of the Commissioner, engaging in and promoting community education and consultation in relation to the protection of individual privacy.[24]

6.19 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,[25] and the 25th International Conference of Data Protection and Privacy Commissioners in 2003–04.[26] The Advisory Committee has also provided input into the guidelines developed by the OPC, as well as advice about the OPC's complaints processes and the publication of complaint case notes.[27]

Composition

6.20 A majority of the Advisory Committee must be persons who are neither officers nor employees, nor members of the staff of an authority or instrumentality, of the Commonwealth.[28] Of the appointed members, the *Privacy Act* specifies that at least one member must have a minimum of five years high level experience in industry, commerce, public administration or government service; one must have a minimum of five years experience in the trade union movement; one must have extensive experience in electronic data-processing; one must be appointed to represent general community interests, including social welfare; and one must have extensive experience in the promotion of civil liberties.[29]

---

22 Ibid s 44(5).
23 Ibid s 82(1)–(5). See also s 87 regarding meetings of the Advisory Committee.
24 Ibid s 83.
25 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 29.
26 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 47.
27 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.
28 *Privacy Act 1988* (Cth) s 82(6).
29 Ibid s 82(7).

6.21 The Advisory Committee currently comprises the Commissioner and five members.[30] Previous members 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.

6.22 Members must disclose any pecuniary interest in a matter being considered by the Advisory Committee that could conflict with the proper performance by a member of his or her functions.[31] Members are liable to removal by the Governor-General in certain events (eg bankruptcy) and may also resign.[32]

Previous inquiries

6.23 In the OPC review of the private sector provisions of the *Privacy Act* (OPC Review), the OPC recommended that:

> The Australian Government should consider changing, by legislative amendment, the name of the Office of the Privacy Commissioner to the Australian Privacy Commission.[33]

6.24 The reason was that the similar names of the Commonwealth, New South Wales and Victorian privacy commissions creates confusion. In addition, the new name would be more consistent with the naming of other federal regulators.[34]

6.25 Other aspects of the OPC discussed above, including the Advisory Committee, did not draw comment in the OPC Review or the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Senate Committee privacy inquiry).

Question 6–1 Is the legislative structure pertaining to the Office of the Privacy Commissioner established under the *Privacy Act* appropriately meeting the needs of the community?

Question 6–2 Are the constraints imposed in the *Privacy Act* on the exercise by the Privacy Commissioner of powers conferred by the Act appropriate?

---

30 See Office of the Privacy Commissioner, *Privacy Advisory Committee* <www.privacy.gov.au/act/pac> at 8 August 2006. Ch 3 discusses the current Advisory Committee.

31 *Privacy Act 1988* (Cth) s 86.

32 Ibid s 85.

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 6.

34 Ibid, 47.

Question 6–3 Does the Privacy Advisory Committee perform a useful role and have appropriate powers and functions? Are the fields of expertise represented on the Privacy Advisory Committee appropriate? Does the Privacy Advisory Committee, and the fields of expertise of Privacy Advisory Committee members, need to be set out in the *Privacy Act*?

Question 6–4 Is the scope of immunities conferred on: (a) the Privacy Commissioner and his or her delegates; (b) an adjudicator appointed under a privacy code and his or her delegates; and (c) other persons, appropriate?

Oversight powers

6.26 The Commissioner has general powers to oversee the operation of the *Privacy Act*. It is generally the Commissioner's sole decision whether a particular power or authority is to be exercised. The general oversight powers relate to the giving of advice, research and monitoring of technological developments, and education.

Advice powers

6.27 The Commissioner has several advisory functions under the *Privacy Act*. These are to advise on:

- matters relevant to the operation of the *Privacy Act*;
- proposals for data-matching or data linkage;
- proposed enactments; and
- the need for legislative or administrative action.

6.28 In addition, the Commissioner has power to provide advice to tax file number recipients and adjudicators, as discussed below.

Advice on matters relevant to the operation of the Act

6.29 The Commissioner may provide advice to a Minister, agency or organisation on any matter relevant to the operation of the *Privacy Act*.[35] A related function is, whenever the Commissioner thinks it necessary, to inform the Minister of action that needs to be taken by an agency in order to achieve compliance by the agency with the IPPs.[36]

---

35 *Privacy Act 1988* (Cth) s 27(1)(f).

36 Ibid s 27(1)(j). The relevant Minister is the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004, pt 2.

Advice on proposals for data-matching or data linkage

6.30 The Commissioner is to examine a proposal for data-matching or data linkage that may involve an interference with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals, and to ensure that any adverse effects of such proposal on the privacy of individuals are minimised.[37]

Advice on proposed enactments

6.31 The Commissioner is to examine a 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 have any adverse effects on the privacy of individuals. The Commissioner is to ensure that any adverse effects of such proposed enactment on the privacy of individuals are minimised.[38]

6.32 A document prepared as the result of such examination is popularly known as a 'privacy impact statement' or 'privacy impact assessment'. As is the case with most of the powers inherent in the functions of the Commissioner established by the *Privacy Act*, the power to examine a proposed enactment and advise on it is relatively wide. It does not require, however, that a Minister obtain a privacy impact assessment, or that any assessment that is obtained be acted on.[39]

6.33 It has been suggested that privacy impact assessments should be required for all proposed Commonwealth legislation, or all proposed Commonwealth legislation carrying a high risk of infringing privacy rights created by the *Privacy Act*.[40] If that suggestion were adopted, the issue arises as to whether the task should be performed by the OPC, some other public officer (currently existing or not), or a private sector individual or organisation. A related question is whether all privacy impact assessments should be subject to the same requirements (including as to whom should complete the task).

6.34 The OPC Review raised the possibility that private sector organisations that develop and implement 'large scale high privacy risk' technology should be

---

37 *Privacy Act 1988* (Cth) s 27(1)(k).

38 Ibid s 27(1)(b).

39 Note however that 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 if the legislation has implications for the privacy of individuals'.

40 Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

encouraged to conduct privacy impact assessments.[41] The OPC has recently released guidelines for agencies in this regard, and the same approach could be applied to organisations.[42] The OPC Review did not go further to discuss whether organisations planning large scale high privacy risk projects should be *required* to prepare, or obtain, a privacy impact assessment, or whether privacy impact assessments are desirable or should be required other than in relation to technology. However, the Senate Committee privacy inquiry recommended that the *Privacy Act* 'be amended to include a statutory privacy impact assessment 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'.[43]

Advice on the need for legislative or administrative action

6.35 It is the Commissioner's function to 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.[44]

Tax file numbers

6.36 The Commissioner also has the power to provide advice, whether requested or not, to tax file number recipients about their obligations under the *Taxation Administration Act 1953* (Cth) and on any matter relevant to the operation of the *Privacy Act*.[45]

Privacy codes

6.37 The Commissioner has the power, on request by the adjudicator, to give 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.[46]

---

41 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 256. This possibility was also discussed in the following consultations: Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006; R Clarke, *Consultation PC 14*, Canberra, 30 March 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006.

42 See Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006).

43 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 5. It is not clear whether this relates to agencies and/or organisations. The OPC has defined 'project' to include 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 understands 'developments' to refer to new technological developments, such as biometrics.

44 *Privacy Act 1988* (Cth) s 27(1)(r). The relevant Minister is currently the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004, pt 2.

45 *Privacy Act 1988* (Cth) s 28(1)(g).

46 Ibid s 27(1)(fa).

Previous inquiries

6.38 The OPC Review 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'.[47] However, it recognised that 'organisations need more guidance'.[48] This raises issues about the adequacy of the OPC's resources, and related issues concerning the OPC's approach to administering the *Privacy Act*. These issues are discussed later in this chapter.

Research and monitoring powers

6.39 The second aspect of the OPC's powers to oversee the *Privacy Act* is in relation to research and monitoring. The Commissioner has the function to undertake research into, and to monitor developments in, 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. The Commissioner is to report to the Minister about the results of such research and monitoring.[49]

6.40 The Commissioner also has the function to monitor and report on the adequacy of equipment and user safeguards.[50] There is very little commentary on this function and it is not clear what equipment and user safeguards are monitored.

Education powers

6.41 It is the Commissioner's function to promote an understanding and acceptance of the IPPs and NPPs and of the objects of those principles.[51] It is also a function of the Commissioner, for the purpose of promoting the protection of individual privacy, to undertake educational programs on the Commissioner's own behalf or in cooperation with other persons or authorities acting on behalf of the Commissioner.[52]

6.42 As noted above, the OPC has said a factor likely to increase 'community confidence that individuals' rights are protected' is 'raising awareness about individuals' privacy rights'.[53] To this end, the OPC provides information through its information hotline and its web site (which contains various OPC publications).

---

47 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 5.
48 Ibid, 7.
49 *Privacy Act 1988* (Cth) s 27(1)(c). The relevant Minister is currently the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004, pt 2.
50 *Privacy Act 1988* (Cth) s 27(1)(q).
51 Ibid s 27(1)(d).
52 Ibid s 27(1)(m).
53 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 105.

6.43 Considerable attention was given to the Commissioner's education power and concerns about transparency and accountability in submissions to the OPC Review and Senate Committee privacy inquiry. Submissions made to the OPC Review took a range of positions on education, some asserting that there is insufficient awareness of individuals' privacy rights in the community, others suggesting that there is sufficient awareness.[54] Overall, the submissions acknowledged that education plays a vital part in community awareness of privacy laws.

6.44 Several submissions suggested public awareness be raised, using either one-off or regular campaigns. Suggestions were also made 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, and that extra funding was needed to exercise fully the Commissioner's educational powers.[55] Publication of more case notes was emphasised as a necessary step.[56]

6.45 A technique for raising awareness of privacy laws that was discussed by the OPC Review is to develop a privacy logo that the Commissioner could authorise organisations to use, as an indication of the organisations' 'commitment to good privacy practice'.[57] This was not the subject of any recommendation. The OPC Review did recommend, however, that:

> The Australian Government should consider specifically funding the Office to undertake a systematic and comprehensive education program to raise community awareness of privacy rights and obligations.[58]

6.46 The OPC also undertook to continue collecting demographic information on complainants to identify and remove any barriers preventing sectors of the community from knowing about and exercising their privacy rights.[59]

6.47 Submissions to this Inquiry suggest that difficulties arise in daily life where a request for information or assistance from an organisation or agency is refused on the ground that the *Privacy Act* prohibits the information or assistance being given, when

---

54 See Ibid, 107–111.

55 Ibid, 107–111.

56 Ibid, 142–143, 151–152. See Office of the Privacy Commissioner, *Complaint Case Notes and Complaint Determinations* <www.privacy.gov.au/act/casenotes/index.html> at 16 August 2006.

57 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 111.

58 Ibid, Rec 26. The ALRC understands that the Australian Government provided some additional funding to the OPC as part of the 2006–07 budget, some of which may be used by the OPC for the purpose of community education. See also Rec 48.

59 Ibid, Rec 27. The ALRC understands that since December 2004, the OPC has routinely invited all complainants to complete a demographic survey.

in truth the Act does not.[60] It is not clear to what extent, if any, spurious or mistaken reliance on the Act can be attributed to a misunderstanding of the Act.

Question 6–5 Are the Privacy Commissioner's powers to oversee the *Privacy Act* appropriate and exercised effectively? For example, are the Commissioner's powers: (a) to furnish advice; (b) to research and monitor developments in data processing and computer technology; (c) to promote understanding of the IPPs and of the objects of the IPPs and the NPPs; (d) to undertake education programs to promote individual privacy protection; (e) relating to tax file numbers; (f) arising under other Acts, appropriate and exercised effectively?

Question 6–6 Should the *Privacy Act* require a privacy impact assessment to be prepared for: (a) all proposed Commonwealth legislation; (b) other proposed projects or developments of agencies; or (c) other proposed projects or developments of organisations?

Question 6–7 If privacy impact assessments are required:

(a) who should be involved in preparing the assessments;

(b) who should be entitled to view the results of the assessments;

(c) who should bear the cost of the assessments; and

(d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

Publication of records

6.48 The Commissioner maintains, and publishes annually, a record (known as the Personal Information Digest) of 'the matters set out in records maintained by record-keepers in accordance with clause 3 of IPP 5'.[61] The matters in IPP 5 are the:

- nature of the records of personal information kept by or on behalf of the record-keeper;

60 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.

61 *Privacy Act 1988* (Cth) s 27(1)(g).

- purpose for which each type of record is kept;
- 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.

6.49 The aim of the Personal Information Digest was evidently to assist individuals to know what information is held about them by agencies, thereby helping the individuals to decide if they need to seek access to and correction of the information.

Question 6–8 Is the Personal Information Digest published in a useful manner? If not, how might it be improved? Is the record itself useful?

General compliance powers

6.50 The Commissioner has general powers to monitor and promote compliance with the *Privacy Act*.[62] These general powers include:

- powers to issue guidelines about how privacy laws operate in particular circumstances or in relation to particular information, both under the *Privacy Act* and other legislation;
- powers to audit agencies regarding their compliance with the Act;
- powers relating to tax file numbers;[63]
- powers relating to credit reporting;[64] and
- other powers conferred by other Acts.

---

62 Powers in relation to complaint-handling are discussed below.
63 Tax file numbers are considered further in Ch 12.
64 Aside from some limited references, the credit reporting provisions of the *Privacy Act* will be considered in a separate Issues Paper.

Guidelines

Generally

6.51 The Commissioner has the power to formulate and issue guidelines under the *Privacy Act*. These are to be published in such manner as the Commissioner considers appropriate and are to assist in 'the avoidance of acts or practices of an agency or an organisation that may or might be interferences with the privacy of individuals or which may otherwise have any adverse effects on the privacy of individuals'.[65]

Privacy codes

6.52 Specific provision is made for the Commissioner to prepare, and to publish in the way that the Commissioner considers appropriate, guidelines regarding privacy codes. These may be to assist organisations to develop privacy codes or to apply approved privacy codes; may relate to making and dealing with complaints under approved privacy codes; or may discuss matters the Commissioner may consider in deciding whether to approve a privacy code or a variation of an approved privacy code.[66] The OPC published Guidelines on Privacy Code Development in September 2001.[67] Other powers concerning privacy codes are discussed later in this chapter.

Tax file numbers

6.53 The Commissioner is vested with special functions in relation to tax file numbers (TFNs). Most of these hinge on s 17—'Guidelines relating to tax file number information'—which provides that the Commissioner must issue written guidelines concerning the collection, storage, use and security of TFN information. The Commissioner has a general power to evaluate compliance with issued TFN guidelines.[68] There are also more specific powers to investigate acts or practices of TFN recipients that may breach any such guidelines[69] and to audit records of TFN information maintained by TFN recipients to ascertain whether the records are maintained according to TFN guidelines.[70] The OPC issued Tax File Number

---

65 *Privacy Act 1988* (Cth) s 27(1)(e). Ch 8 considers the Commissioner's power to approve medical research guidelines and guidelines about health information issued by the CEO of the National Health and Medical Research Council pursuant to *Privacy Act 1988* (Cth) ss 95, 95A.

66 *Privacy Act 1988* (Cth) s 27(1)(ea).

67 Office of the Federal Privacy Commissioner, *Guidelines on Privacy Code Development* (2001). The OPC has undertaken to 'review the Code Development Guidelines dealing with the processes relating to code approval with a view to simplifying them': 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.

68 *Privacy Act 1988* (Cth) s 28(1)(f).

69 Ibid s 28(1)(b).

70 Ibid s 28(1)(e). The OPC has published a manual which sets out the policies and process adopted by the OPC for the performance of privacy audits of tax file number information: Office of the Privacy Commissioner, *Privacy Audit Manual—Part II (Tax File Number Guidelines)* (1995).

Guidelines in 1992 and it publishes an annotated version of the Guidelines (including all amendments as at March 2004) on its website.[71]

Other legislation

6.54 The Commissioner is specifically given the power to formulate and issue guidelines under other legislation: namely s 12 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and s 135AA of the *National Health Act 1953* (Cth).[72]

Nature and utility of guidelines

6.55 In the OPC Review considerable attention was given to solving 'systemic issues' of privacy compliance and non-compliance. The OPC defined 'systemic issues' to mean 'issues that are about an organisation's or industry's practice rather than about an isolated incident';[73] the key element here apparently being repetition. As discussed in more detail below, concerns were raised in consultations and submissions that the Commissioner is not treating systemic issues effectively or is unable to deal with systemic issues properly by using existing powers. The OPC Review recommended that the Government consider amending the *Privacy Act* to provide a power to develop and issue binding guidelines (and/or binding codes, which are discussed below) in cases where there is a strong public interest, where more detailed guidance is warranted or complaints reveal recurrent breaches.[74]

6.56 The OPC Review considered that binding guidelines should be: disallowable instruments for the purposes of the *Acts Interpretation Act 1901* (Cth); drafted after consultation with affected stakeholders; and take into account any potential negative impact if they were to be issued. The OPC said a power to issue binding guidelines

> 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. This [would create] a more level playing field among organisations, and [would ensure] that conscientious organisations are not commercially disadvantaged.
>
> Such 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

---

71 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992). The regulation of TFNs is discussed in Ch 12.

72 *Privacy Act 1988* (Cth) ss 27(1)(p), 27(1)(pa). See the Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997); 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 Medicare and Pharmaceutical Guidelines are discussed in Ch 8.

73 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.

74 Ibid, Rec 44.

uncertainty in application of NPPs in particular situations. It would also benefit consumers to have a more specific idea of their rights.[75]

6.57 The ALRC is interested in views on whether the Commissioner should have power to issue binding guidelines, and if so, in what circumstances.

Audit powers

6.58 The *Privacy Act* confers audit powers on the Commissioner in relation to agencies. There are powers to:

- conduct audits of records for the purpose of ascertaining whether agencies' records are maintained according to the IPPs;[76] and

- conduct audits of particular acts done, and particular practices engaged in, by agencies in relation to personal information, if those acts and practices, and those agencies, are prescribed by regulations.[77]

6.59 Organisations are only subject to audit by the Commissioner under powers associated with the TFN and credit reporting provisions.[78] There is no general power to audit the privacy compliance of organisations, although if an organisation requests it, 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 according to either an approved privacy code or the NPPs, as applicable.[79] As at the date of the OPC Review, the Commissioner had not conducted any audits under this power.[80]

6.60 There were many submissions to the OPC Review and Senate Committee privacy inquiry that stated that the NPPs should be amended to confer an audit power on the Commissioner.[81] One participant in the OPC Review commented that if the Commissioner had audit powers, 'we might be able to convince our boards to comply

---

75 Ibid, 158.

76 *Privacy Act 1988* (Cth) s 27(1)(h). The OPC has published a Privacy Audit Manual for this purpose: Office of the Privacy Commissioner, *Privacy Audit Manual—Part I (Information Privacy Principles)* (1995).

77 *Privacy Act 1988* (Cth) s 27(1)(ha).

78 Ibid ss 28(1)(e), 28A(1)(g). See also Office of the Privacy Commissioner, *Privacy Audit Manual—Part II (Tax File Number Guidelines)* (1995).

79 *Privacy Act 1988* (Cth) s 27(3).

80 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 157.

81 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*]'.[82] Others expressed the view that an extended audit power is necessary to maintain public confidence in the Commissioner's role.[83]

6.61 It has been suggested to the ALRC that the Commissioner's audit powers be supplemented by requiring every regulated private sector organisation to audit its own compliance with the *Privacy Act*.[84] The *Corporations Act 2001* (Cth) model of financial reporting and audits is 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.[85] The Commissioner could also have the power to audit such organisations as the Commissioner chooses, without being required to audit every organisation. Civil and possibly criminal sanctions could apply if the reporting or auditing obligation of the organisation is not fulfilled properly.

6.62 The possibility of self-audits raises the related issue of whether companies who are subject to a self-audit, reporting and OPC auditing regime should receive some immunity or benefit. This might consist of a statutory letter of comfort, which could potentially be used as evidence that the company has an approved compliance program in place. If the audit process revealed some kind of systemic issue (or any privacy issue), the company would not receive the immunity or benefit until the issue had been resolved to the satisfaction of the Commissioner. This process could also pick up on the idea of a privacy logo, discussed above.

6.63 The OPC Review canvassed the possible expansion of the Commissioner's audit powers, but ultimately did not recommend that the Commissioner be given the power to audit private sector organisations. The OPC Review recognised that such a power may increase community confidence in the *Privacy Act* and help to identify and monitor responses to systemic issues. It noted, however, that such a power has resource implications and that the role might be filled better by private sector consultancy firms.[86]

---

82 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 133. See also N Waters, *Consultation PC 17*, Sydney, 2 May 2006.

83 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 145.

84 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.

85 A stakeholder to the Senate Committee privacy inquiry suggested a 'self-audit-self-regulatory process' as a more efficient way to deal with complaints: see Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.21].

86 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 157.

6.64 The OPC Review suggested that a more appropriate role for the OPC would be to educate organisations on the value of audits.[87] To this end, the OPC recommended that it would

> consider promoting privacy audits by private sector organisations, including 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 for organisations.[88]

6.65 In contrast to the OPC Review, the Senate Committee privacy inquiry urged the introduction of private sector auditing powers for the OPC.[89]

Question 6–9 What powers should the Privacy Commissioner have to audit agencies and organisations?

Question 6–10 Should organisations and agencies be required to self-audit periodically to ensure and to demonstrate compliance with the *Privacy Act*?

Powers under other Acts

6.66 The Commissioner is required to formulate guidelines under the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the *National Health Act 1953* (Cth). These Acts also provide the Commissioner with investigative and enforcement functions in relation to these guidelines. In addition, the Commissioner has a number of functions under the *Telecommunications Act 1997* (Cth) and the *Crimes Act 1914* (Cth). One issue for consideration is whether these functions should be consolidated under the *Privacy Act*.

Data-matching Program (Assistance and Tax) Act 1990 (Cth)

6.67 The Commissioner first issued the *Data-matching Program (Assistance and Tax) Guidelines* in September 1991.[90] Under s 13 of the *Data-matching Act* the Commissioner has the power to investigate any act or practice that appears to breach the Act or Data-Matching Guidelines. Where the Commissioner finds a breach he or she must endeavour to make satisfactory arrangements with the agency about the act or practice. Where satisfactory arrangements are not in place, or the Commissioner

87 See Ibid, 157.
88 Ibid, Rec 39.
89 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.56].
90 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. The *Data-Matching Act* is discussed further in Ch 7.

considers it appropriate in all the circumstances, the Commissioner must make a report about the act or practice to the Minister for Family, Community Services and Indigenous Affairs. If after a period of time the Commissioner is not satisfied that an agency has taken reasonable steps to prevent a repetition of the act or practice, the Commissioner can give a further report to the Minister who must lay it in each House of Parliament within 15 sitting days.[91]

6.68 When conducting an investigation under the *Data-matching Act*, the Commissioner has all the powers of investigation that he or she has under Part V and s 99 of the *Privacy Act*.[92] Nothing in the *Data-matching Act* limits the rights of persons under the *Privacy Act* to complain to the Commissioner about an interference with privacy.[93]

National Health Act 1953 (Cth)

6.69 Section 135AA of the *National Health Act 1953* (Cth) requires the Commissioner to issue guidelines in relation to the handling of information obtained by an agency in connection with a claim for payment of a benefit under the Medicare Benefits Program or the Pharmaceutical Benefits Program. The *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines* address a number of issues, including: the ways in which Medicare Benefits Program information and Pharmaceutical Benefits Program information is to be stored, used, disclosed and destroyed; and the prohibition of linkage of information that is held in a database maintained for the purposes of the Medicare Benefits Program and the Pharmaceutical Benefits Program.[94]

6.70 A breach of the Guidelines constitutes an interference with privacy for the purposes of the *Privacy Act*.[95] An individual may complain to the Commissioner under s 36 of the *Privacy Act* about a practice that may be a breach of the Guidelines. A complaint concerning a breach of the Guidelines will be dealt with in the same way as a complaint about a breach of an IPP.[96]

Telecommunications Act 1997 (Cth)

6.71 Part 6 of the *Telecommunications Act 1997* (Cth) provides for the development of industry codes and standards for telecommunications industry activities. The Commissioner must be consulted about industry codes and standards that deal with

---

91 *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 13.
92 Ibid s 13(7).
93 Ibid s 13(8). A breach of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) or Guidelines constitutes an interference with privacy under s 13 of the *Privacy Act*: *Privacy Act 1988* (Cth) s 13(ba).
94 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.
95 *National Health Act 1953* (Cth) s 135AB; *Privacy Act 1988* (Cth) s 13(bb).
96 For further discussion of the *National Health Act 1953* (Cth), see Ch 8.

privacy issues.[97] The Commissioner must also be consulted: before the Australian Communications and Media Authority enforces an industry code relating to a matter dealt with by the NPPs or an approved privacy code;[98] 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.[99]

6.72 Part 13 of the *Telecommunications Act 1997* regulates the use and disclosure of information obtained by certain bodies during the supply of telecommunication services. In particular, Part 13 requires carriers, carriage service providers and number database operators to create records of certain disclosures of protected information.[100] Section 309 of the *Telecommunications Act 1997* requires the Commissioner to monitor compliance with the record keeping requirements under the Act. The Commissioner may give the Minister for Communications, Information Technology and the Arts a written report about any matters arising out of the performance of the function.[101]

Crimes Act 1914 (Cth)

6.73 Part VIIC of the *Crimes Act 1914* (Cth) provides for a spent convictions scheme that prevents discrimination against individuals on the basis of certain previous convictions. An individual's conviction for an offence is 'spent' if: the individual has been granted a pardon for a reason other than the person was wrongly convicted of the offence; or the individual was not sentenced to imprisonment or was imprisoned for a period not more than 30 months and the waiting period for the offence has ended.[102] The spent convictions scheme allows individuals with certain convictions to disregard those convictions after a specified period.[103] In addition, the law prohibits taking these convictions into account, or disclosing them to anyone without the consent of the individual.[104] Part VIIC of the *Crimes Act* also applies to pardons and convictions that have been quashed.[105]

6.74 The Commissioner has the power to investigate complaints about breaches of Part VIIC of the *Crimes Act*.[106] If the Commissioner finds a complaint substantiated he

---

97 *Telecommunications Act 1997* (Cth) ss 117(1)(j), 117(1)(k), 118, 134. In 2004–05, the Privacy Commissioner provided advice on privacy issues in respect of 17 codes being developed pursuant to the *Telecommunications Act 1997* (Cth): Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), [1.8.1].

98 *Telecommunications Act 1997* (Cth) ss 121, 122.

99 Ibid s 282(8).

100 Ibid s 306.

101 For a more detailed discussion of the *Telecommunications Act 1997*, see Ch 10.

102 *Crimes Act 1914* (Cth) s 85ZM. A 'waiting period' is five years if the person was dealt with as a minor in relation to a conviction, and 10 years in any other case: *Crimes Act 1914* (Cth) s 85ZL.

103 *Crimes Act 1914* (Cth) ss 85ZV, 85ZW.

104 Ibid s 85ZW(b).

105 Ibid pt VIIC, div 2.

106 Ibid ss 85ZZ, 85ZZC.

or she can make a determination and certain orders, including the payment of compensation.[107] The Commissioner also has responsibility for assessing applications for complete or partial exclusions from the requirements of the scheme and recommending to the Attorney-General whether an exclusion should be granted, and what conditions should apply.[108]

6.75 In 2001, the Standing Committee of Attorneys-General (SCAG) established a Working Party to consider issues related to the spent convictions scheme. A discussion paper entitled *Uniform Spent Convictions: A Proposed Model* was prepared in 2004 and is the subject of ongoing discussion by SCAG.[109] In this Inquiry the ALRC's consideration of the spent convictions scheme will be limited to the functions of the Commissioner under Part VIIC of the *Crimes Act 1914* (Cth).

Question 6–11 Should all the Privacy Commissioner's functions be consolidated in the *Privacy Act?*

Complaint-handling powers

6.76 A complaint is a formal allegation by a complainant that there has been an interference with his or her privacy by an agency or organisation.[110] The *Privacy Act* provisions on the topic are detailed.

6.77 The *Privacy Act* requires or permits various steps to be taken at different stages by a complainant, the respondent, certain interested parties, and the Commissioner. Not all these steps must be taken for the resolution of any given complaint. For example, the Commissioner may conduct preliminary investigations into a complaint and afterwards dismiss it for lack of substance. Complaints that proceed past the preliminary stage may be withdrawn or resolved between the complainant and respondent, removing the need for intervention by the Commissioner.

6.78 Where the Commissioner does act to resolve a complaint, he or she may act informally, by conciliating the dispute, and take no further formal steps. However, the Commissioner may also take the further step, after investigating a matter, of making a determination in the dispute. The determination may include a declaration that the complainant's rights under the *Privacy Act* have or have not been infringed. A declaration can also be made that a complainant is entitled to be paid compensation,

---

107 Ibid ss 85ZZD–85ZZE.

108 Ibid s 85ZZ(1)(b).

109 Victorian Government Department of Justice, *Uniform Spent Convictions: A Proposed Model*, Discussion Paper (2004). See also K Curtis, 'Access and Privacy: Getting the Balance Right' (Paper presented at Australian Court Administrators Group—Courts and Tribunals Annual Conference, Sydney, 25 November 2005), 9.

110 *Privacy Act 1988* (Cth) s 36(1).

though the legal effect of such a declaration depends on whether the respondent is an agency or organisation. Determinations can be enforced in the Federal Magistrates Court or the Federal Court of Australia.

6.79 The OPC Review reported that the OPC currently receives approximately 1250 complaints per year.[111] Generally, the OPC seeks to resolve disputes informally between the parties through conciliation. Typical outcomes involve the respondent:

- apologising to the complainant;
- giving the complainant access to his or her record, or amending the record;
- changing its practices or procedures;
- training its staff in a relevant way; and
- paying compensation or taking other remedial steps to redress actual loss or damage suffered by the complainant.[112]

6.80 The OPC Review noted that 'to date, the Office has 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''.[113] This is an important comment in that it illustrates the OPC's current approach.

6.81 It is necessary for the purposes of this Inquiry to consider on two levels the handling of complaints. On one level, it is necessary to consider individually the elements and processes in the making of a complaint. This is particularly so because complaints are not treated uniformly under the *Privacy Act*. The second level is concerned with how the system as a whole is operating, which will be considered in the 'Compliance models' section of this chapter.

6.82 Focusing on the individual elements and processes in the making of a complaint, the discussion will first look at the source of the Commissioner's powers regarding complaints, before turning to how complaints are commenced, and the steps that can be taken from there.

---

111 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 126.
112 Ibid, 126.
113 Ibid, 126.

Complaint process

Source of powers

6.83 Powers to investigate and conciliate complaints under the IPPs and the NPPs are established in separate paragraphs of s 27(1).[114] The trigger that enlivens these powers is that a 'complaint' is made. The definitions of 'agency' and 'organisation' operate so that the two sources of power operate in different fields. Complaints under approved privacy codes are discussed later in the chapter.

Making a complaint

6.84 Broadly, 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*.[115] The Commissioner is generally required to investigate an act or practice if the act or practice may be an interference with an individual's privacy and a complaint has been made about the act or practice.

6.85 In some situations, however, the Commissioner is prohibited from investigating a matter, or has power to decide whether to investigate a matter. Further, 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.[116]

6.86 There are certain conditions that must be complied with when making a complaint. For instance, a complaint must be in writing and is to specify the respondent.[117] A complainant is entitled to certain assistance from staff of the OPC in preparing the complaint.[118]

6.87 One of a class of two or more individuals who may have had their privacy interfered with may make a complaint on behalf of all the individuals in the class.[119] There are conditions on the manner of making a representative complaint, including that a representative complaint must describe or identify the class members, specify the

---

114 *Privacy Act 1988* (Cth) ss 27(1)(a), 27(1)(ab).

115 As will be seen, Ibid pt V (headed Investigations) also imposes *obligations* on persons, agencies and organisations in particular circumstances. Regarding organisations, special provisions are made for the application of pt V to partnerships, unincorporated associations, trusts, and former organisations: see Ibid ss 70A, 70B.

116 Ibid s 36(1A). See s 36(1B)–(1C) for exceptions to s 36(1A).

117 Ibid s 36(3), (5). Sections 36(6)–(8) and 37 regulate who is the respondent to various claims where the act or practice is that of an agency or organisation.

118 Ibid s 36(4). A complainant is also entitled to assistance from staff of the Commonwealth Ombudsman, where powers of the Commissioner have been delegated to the Commonwealth Ombudsman under *Privacy Act 1988* (Cth) s 99.

119 *Privacy Act 1988* (Cth) s 36(2).

nature of the complaints, the relief sought and the questions of law or fact that are common to the complaints of the class members.[120]

6.88 The Commissioner has power in certain circumstances to substitute a respondent to a complaint. In particular, where a service provider under a Commonwealth service contract dies, ceases to exist, becomes bankrupt or insolvent, the Commissioner can amend the complaint to make the agency or its principal executive the respondent to the complaint, instead of the organisation.[121]

Costs

6.89 Generally financial assistance is not available to persons wishing to make a complaint. There is no equivalent of a legal aid scheme in this area.[122]

6.90 The OPC does not currently charge complainants fees for handling complaints. The OPC Review discussed cost recovery, but no recommendation was made in this regard.[123]

6.91 One submission to the ALRC Inquiry contended that the current complaint handling system under the *Privacy Act* lacks means of 'accessible, fair and effective dispute resolution'.[124] All aspects of the Commissioner's complaint-handling powers discussed above will be reviewed by the ALRC in the course of this Inquiry and the ALRC is interested in views on the complaint-handling process.

Investigations

6.92 The *Privacy Act* provides for investigations to be conducted by the Commissioner. An investigation may be undertaken because a person has complained that his or her privacy rights under the *Privacy Act* have been infringed. In that case, before commencing an investigation, the Commissioner has power to conduct preliminary inquiries.

6.93 The *Privacy Act* draws a distinction between investigations triggered by a complaint, and those initiated by the Commissioner in the absence of a complaint ('own-motion' investigations). While there are technical differences between the two

---

120 Ibid s 38.

121 Ibid s 50A. The Commissioner has a similar power in relation to determinations: *Privacy Act 1988* (Cth) s 53B.

122 In limited circumstances, there is financial assistance available to persons in connection with a file number complaint that has been dismissed by the Commissioner where the respondent is not an agency or the principal executive of an agency: *Privacy Act 1988* (Cth) s 63. The assistance available is narrow, and reflects a special concern with tax file numbers.

123 See Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 162.

124 Consumer Credit Legal Centre (NSW) Inc, *Submission PR 28,* 6 June 2006.

kinds of investigations, there are set standards and rules applying to all investigations. Generally, the Commissioner will comply with any published guidelines on investigations.

Preliminary inquiries

6.94 Where a complaint is made to the Commissioner or the Commissioner accepts a complaint referred to him or her by the adjudicator under a privacy code,[125] the Commissioner has the power to make preliminary inquiries of the respondent.[126] The power is limited by its purpose, which is to determine whether the Commissioner has power to investigate the matter to which the complaint relates or whether the Commissioner may, in his or her discretion, decide not to investigate the matter.[127]

6.95 Deciding these questions is an important step for two reasons: the Commissioner must not investigate a matter in certain specified circumstances, and in other circumstances, the Commissioner is given the power to decide whether to investigate a matter.

Investigations of complaints

6.96 As suggested above, some matters the Commissioner is required to investigate, others the Commissioner must *not* investigate, while in a third category of circumstances the Commissioner has discretion whether to investigate.

Obligation to investigate

6.97 The Commissioner must investigate an act or practice if the act or practice may be an interference with the privacy of an individual and a complaint has been made about it under s 36.[128]

6.98 However, the Commissioner must not investigate a complaint 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.[129] Two submissions to the OPC Review suggested that this requirement is 'overly bureaucratic'.[130]

Matters Commissioner must not investigate

6.99 In certain situations the Commissioner must not investigate a complaint. For example, if in the course of a s 40 investigation, the Commissioner forms the opinion

---

125 *Privacy Act 1988* (Cth) s 40(1B).
126 Ibid s 42.
127 Ibid s 42.
128 Ibid s 40(1).
129 Ibid s 40(1A).
130 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 139.

that a 'tax file number offence' or a 'credit reporting offence' has been committed,[131] he or she is to 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.[132] 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.[133]

6.100 Similarly, the Commissioner must not investigate a matter that is under investigation by the Auditor-General unless the Commissioner and the Auditor-General agree otherwise. The Commissioner may resume his or her investigation once the Auditor-General's investigation is complete.[134]

Discretion not to investigate or to defer investigation

6.101 The Commissioner may decide not to investigate, or not to investigate further, certain complaints made under s 36,[135] where:

- the act or practice is not an interference with privacy; the act or practice occurred more than 12 months before the complaint was made; 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 under that law; or another law provides a more appropriate remedy for the complaint;[136]

- the 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;[137]

- the 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;[138] or

---

131 These terms are defined in *Privacy Act 1988* (Cth) s 49(4).
132 Ibid s 49(1).
133 Ibid s 49(2)–(3).
134 Ibid s 51.
135 The same provisions apply in relation to complaints referred to and accepted by the Commissioner by an adjudicator under an approved privacy code: Ibid s 40(1B). Referrals are included in the discussion of privacy codes later in the chapter.
136 See Ibid s 41(1).
137 Ibid s 41(2).
138 Ibid s 41(3).

- the Commissioner forms the view that the complaint could have been made to the Human Rights and Equal Opportunity Commission, Commonwealth Ombudsman, Postal Industry Ombudsman, or Public Service Commissioner and would be dealt with more effectively or conveniently by one of those bodies.[139]

Previous inquiries

6.102 The OPC Review recommended that the Australian Government consider amending the *Privacy Act* to confer on the Commissioner power to decide not to investigate a complaint where the harm to individuals was minimal and there would be no public interest in pursuing the matter.[140]

6.103 The recommendation was criticised in a submission to the Senate Committee privacy inquiry on the basis that the Commissioner should not be able 'to pick and choose which complaints to investigate'.[141] It was suggested that the OPC's resources would be consumed by the process of assessing the 'harm' and 'public interest' elements of a complaint rather than just resolving it.[142] The Senate Committee noted these concerns and urged the Australian Government 'to consider carefully the various implications of such an approach'.[143]

6.104 The OPC Review noted that another common concern was the 'lack of a merits-based review process for decisions made under section 41' of the *Privacy Act*, particularly where the Commissioner chooses not to investigate a complaint, even though the complainant might not be satisfied with the respondent's response.[144] On the other hand, others submitted that a lack of appeal rights under the *Privacy Act* was not unique to that legislation, and had not been shown to be problematic.[145]

6.105 The Victorian Law Reform Commission (VLRC) recommended in its 2005 *Workplace Privacy: Final Report* that where a regulator declines a complaint on similar grounds to those set out in s 41(1) of the *Privacy Act*, the regulator be required to notify the complainant and respondent of that fact, and the complainant be able to require the regulator to refer the matter to the Victorian Civil and Administrative

---

139 Ibid s 50. The possibility of improving liaisons with overlapping complaints handlers was discussed in 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.

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 46.

141 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.28].

142 Ibid, [6.28]–[6.30].

143 Ibid, [7.55].

144 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 139. See also Rec 40.

145 Ibid, 139.

Tribunal for a hearing.[146] The ALRC is interested in views as to whether a similar provision should be included in the *Privacy Act*.

Own-motion investigations

6.106 The Commissioner may investigate an act or practice without a complaint having been made if the act or practice may be an interference with the privacy of an individual and the Commissioner thinks it is desirable that it be investigated.[147] These investigations are known colloquially as 'own-motion' investigations.[148]

Systemic issues

6.107 The OPC Review and Senate Committee privacy inquiry received submissions noting that systemic issues arise in privacy compliance which the Commissioner is not dealing with either because:

- the Commissioner lacks appropriate powers; or
- while having powers to deal with systemic issues, the Commissioner does not exercise them at all or to the requisite degree; or
- the outcome of exercising a power—such as making a determination—is not an effective way to solve systemic issues.[149]

6.108 Stakeholders also raised concerns about the lack of information provided when systemic issues were raised with the OPC.[150]

6.109 Systemic issues emerged as a significant topic in the OPC Review and will be significant in this Inquiry. The discussion of systemic issues raises three questions: what are the systemic issues being discussed; what powers does the Commissioner have to address systemic issues; and, so far as the Commissioner has powers to address systemic issues, are the powers being applied effectively? The ALRC is interested in hearing from stakeholders about these issues.

---

146 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.58]. This approach is taken in the *Information Privacy Act 2000* (Vic) s 29(2) and the *Health Records Act 2001* (Vic) s 51(2).

147 *Privacy Act 1988* (Cth) s 40(2).

148 The procedural conduct of own-motion investigations is largely the same as for investigations of complaints. The investigation of complaints is discussed below.

149 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 134–137. The Investment and Financial Services Association and Telstra opposed these submissions: Ibid, 137.

150 Ibid, 135. See also Rec 38.

Features of systemic issues

6.110 As noted earlier when discussing guidelines, the OPC Review defined systemic issues to mean 'issues that are about an organisation's or industry's practice rather than about an isolated incident'.[151] The definition raises two points.

6.111 First, the distinction between a practice of an organisation, industry or agency[152] and an isolated incident of interference with an individual's privacy under the *Privacy Act* is not stark. An act or practice of an agency or organisation may interfere with an individual's privacy under the Act while appearing to be an isolated incident of non-compliance with the Act.

6.112 Secondly, whether an interference with an individual's privacy is viewed as isolated depends on the factor used to test whether there is linkage between several interferences with individuals' privacy. A thorough understanding of the nature of the business, administrative and other systems used by an organisation, agency, industry or industry sector to conduct its affairs can show that interferences with individuals' privacy that might otherwise be thought to be isolated are in fact related by some feature of the relevant system. In that sense, what might appear to be isolated interferences with privacy may on further examination be shown to be systemic. Further, while the activities of large organisations or agencies may be thought to raise the greatest number of systemic issues, the activities of small organisations or agencies may equally raise systemic issues.

6.113 It follows that systemic issues can refer to a range of potentially disparate activities. Analysis of the Commissioner's ability to deal with these issues, and how the Commissioner currently approaches them, therefore depends on the precise nature of the problem. The ALRC is interested in identifying what constitutes a systemic issue, as effective reforms of existing law or practice can only be made by identifying precisely those features.

Existing powers to address systemic issues

6.114 Section 52 of the *Privacy Act*—'Determination of the Commissioner'—allows the Commissioner to declare that the respondent has engaged in conduct constituting an interference with the privacy of an individual and that the respondent should not repeat or continue such conduct.

6.115 The OPC Review noted that the complaint-handling mechanism is of limited use in resolving systemic issues.[153] It noted that a determination under s 52 'cannot require

---

151 Ibid, 130 fn 102.

152 The OPC Review did not include agency in its definition because it was reviewing only the private sector provisions. However, the definition can equally be applied to agencies.

153 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 134. See also Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.30].

a respondent to do something or refrain from doing something unless the activity relates to matters raised by the complainant'.[154]

6.116 If the conduct affects more than one individual, the Commissioner has the power to add the individual complaint to an existing representative complaint.[155] However, as with an individual complaint, the Commissioner only has the power to find that a respondent has engaged in conduct constituting an interference with the privacy of individuals who are members of the representative complaint and that the respondent should not repeat or continue that conduct. The Commissioner does not have any other power to prescribe how the respondent should act.[156]

6.117 The OPC Review found that 'the overall view from consumer/privacy advocate submissions is that representative complaints, whilst useful in raising systemic issues, were not viewed as being effective in addressing broader systemic issues' because the *Privacy Act* does not provide the Commissioner with power to enforce systemic remedies.[157]

6.118 Another possible way of addressing systemic issues is for the Commissioner to commence a separate own-motion investigation into the matters emerging from the individual complaint while maintaining the confidentiality of the individual complaint under s 40(2). Conducting a separate investigation could, however, involve the doubling up of work and expense.[158]

6.119 In the OPC Review, the OPC recommended that it would 'consider options for providing more feedback on systemic issues either in advice or guidance or in some form of regular update to stakeholders'.[159] The OPC Review also recommended that the Australian Government should consider amending the *Privacy Act* to:

- expand the remedies available following a determination under section 52 to include giving the Privacy Commissioner power to require a respondent to take steps to prevent future harm arising from systemic issues

---

154 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 136; Complaint Determinations 1–4 of 2004 at Office of the Privacy Commissioner, *Complaint Case Notes and Complaint Determinations* <www.privacy.gov.au/act/casenotes/index.html> at 16 August 2006.

155 *Privacy Act 1988* (Cth) s 38C.

156 Office of the Federal Privacy Commissioner, *Complaint Determination No 1 of 2004*, 1 April 2004, [98].

157 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 137.

158 See also Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.20]. Note that the Commissioner's powers to make a determination under s 52 do not apply to own-motion investigations.

159 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 38.

- provide for enforceable remedies following own motion investigations where the Commissioner finds a breach of the NPPs.[160]

6.120 The Commonwealth Ombudsman has own-motion investigation powers that are used to deal with systemic issues. The own-motion power in s 5(1)(b) of the *Ombudsman Act 1976* (Cth) confers power on the Ombudsman to, 'of his or her own motion, investigate *any action*, being action that relates to a matter of administration', subject to exceptions in s 5(2).[161] The question arises whether the *Ombudsman Act* provides a better model than that in the *Privacy Act*.

Conduct of investigations

6.121 The standards for conducting own-motion investigations and investigations triggered by complaints are similar, although not identical. Within the area of complaint investigations, the rules vary depending on whether the complaint concerns the IPPs, the NPPs, or a privacy code.

6.122 As a general rule, an investigation is to be 'conducted in private but otherwise in such manner as the Commissioner thinks fit'.[162] Some of the Commissioner's powers and obligations in conducting the investigations are set out below.

- The Commissioner must give the respondent notice of a decision to investigate a complaint[163] and must inform the complainant and respondent if he or she decides not to investigate a matter further or at all.[164]

- The Commissioner does not have to afford a complainant or respondent the opportunity to appear before the Commissioner unless the Commissioner proposes to make a determination that is adverse to the complainant or respondent.[165]

- The Commissioner has power to obtain information and documents from persons, and make inquiries of persons or examine witnesses on oath or affirmation.[166]

---

160 Ibid, Rec 44. See also Ibid, 157. Note that the Senate Committee privacy inquiry considered that the OPC Review's recommendations relating to the powers of the Commissioner should be implemented as soon as possible: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.27], [7.56].

161 Emphasis added. The Ombudsman has a complaint-based power as well: *Ombudsman Act 1976* (Cth) s 5(1)(a).

162 *Privacy Act 1988* (Cth) s 43(2). Similarly, see *Ombudsman Act 1976 (Cth)* s 8(2); *Migration Act 1958* (Cth) s 429.

163 *Privacy Act 1988* (Cth) s 43(1). See also s 43(1A) where the respondent is a contracted service provider.

164 Ibid s 48.

165 Ibid s 43(4)–(6).

166 Ibid ss 43(3), 44–46. The power to obtain information and documents is subject to ss 69–70. It is an offence not to comply with the Commissioner's directions—see *Privacy Act 1988* (Cth) ss 46(2), 65–66.

- The Commissioner has the power to enter premises with consent or a search warrant and may inspect any documents that are kept at those premises, with some exceptions.[167]

- The Commissioner is able to discuss any matter that is relevant to the investigation with a Minister concerned with the matter, except where the investigation concerns an NPP or privacy code complaint.[168]

Reports by the Commissioner

6.123 Following certain own-motion investigations,[169] examinations of proposed enactments[170] and certain audits and monitoring activities,[171] the Commissioner may or must (depending on the circumstances) report to the Minister about specific matters.[172] In certain circumstances, the Commissioner can give a further report to the Minister who must lay it before each House of Parliament within 15 sitting days.[173]

6.124 There is no express power or obligation to report about investigations of complaints[174] and the *Privacy Act* does not explicitly envisage the Commissioner reporting directly to Parliament.[175]

Question 6–12 Are the procedures under the *Privacy Act* for making and pursuing a complaint, including a representative complaint, appropriate? Are the Privacy Commissioner's powers to make preliminary inquiries and investigate complaints appropriate and effective?

Question 6–13 Is the obligation of the Privacy Commissioner to investigate a complaint about an act or practice that may interfere with the privacy of an individual appropriate, and is it administered effectively?

---

167 *Privacy Act 1988* (Cth) ss 68, 70(1)–(2).
168 Ibid s 43(8)–(8A). See also s 43(7).
169 Ibid s 30.
170 Ibid s 31.
171 Ibid s 32.
172 The relevant Minister is currently the Attorney-General of Australia: Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004, pt 2. Certain matters may be excluded from reports—see *Privacy Act 1988* (Cth) s 33.
173 *Privacy Act 1988* (Cth) ss 30(4)–(5), 31(4)–(5), 32(2)–(3).
174 See Ibid s 30(6).
175 The Victorian Privacy Commissioner suggested that the Privacy Commissioner should have power to table reports in Parliament—see Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.38]. 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), 128.

Question 6–14 Is the power of the Privacy Commissioner to investigate an act or practice that may interfere with the privacy of an individual appropriate, and is it used effectively?

Question 6–15 Are the Privacy Commissioner's powers relating to the conduct of investigations appropriate and exercised effectively ? For example, are the Commissioner's powers regarding: (a) appearances before the Commissioner; (b) conferences; (c) obtaining information and documents; (d) examining witnesses; (e) entering premises to gather information; (f) discussion of complaints with a Minister or other designated person; and (g) reports, appropriate and exercised effectively?

Determinations following investigation of complaints

6.125 The *Privacy Act* allows for two kinds of determinations. The first is a determination in response to a complaint by an individual that his or her rights to privacy under the Act have been infringed. The second is a public interest determination, which is discussed separately below.

6.126 In relation to the former, after investigating a complaint the Commissioner may make a determination dismissing the complaint. Alternatively, he or she can find the 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;[176]
- the respondent should perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;[177]
- the complainant is entitled to a specified amount by way of compensation for any loss or damage;[178] or
- it would be inappropriate for any further action to be taken in the matter.[179]

---

176 *Privacy Act 1988* (Cth) s 52(1)(b)(i).

177 Ibid s 52(1)(b)(ii). 'Loss or damage' is defined in s 52(1A).

178 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).

6.127 Where the determination concerns a breach of IPP 7 or NPP 6 (or an equivalent code provision), the Commissioner has power to include an order that the respondent make an appropriate correction, deletion or addition to a record, or attach to a record a statement provided by the complainant of a correction, deletion or addition sought by the complainant.[180]

6.128 A determination of the Commissioner under s 52(1) is not binding or conclusive between any of the parties to the determination.[181] This reflects the fact that Commonwealth judicial power can only be exercised by a court in accordance with Chapter III of the *Australian Constitution*. Key elements of judicial power are that it is 'a binding and authoritative determination of rights, duties and other justiciable claims, by reference to law'.[182]

6.129 There have been eight complaint determinations made in more than 12 years.[183] 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.[184]

6.130 Professor Graham Greenleaf submitted to the OPC Review that a complainant should have the right to compel the Commissioner to make a determination in relation to a complaint.[185] If adopted in the legislation, this would remove the discretion of the Commissioner to decide whether to make a determination and may narrow the options available to the Commissioner in deciding how to deal with a complaint. This may reduce the flexibility of the system and encourage formality, which other stakeholders submitted should be minimised in the complaint handling process.[186] As noted earlier, a decision by the Commissioner not to make a determination may be subject to judicial review under the ADJR Act. The ALRC is interested in views on these issues.

---

179 *Privacy Act 1988* (Cth) s 52(1)(b)(iv).

180 Ibid s 52(3A)–(3B). This applies also to credit information files and credit reports, which are to be considered in a separate Issues Paper.

181 Ibid s 52(1B).

182 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 and, especially, *Brandy v Human Rights and Equal Opportunity Commission* (1995) 183 CLR 245.

183 Office of the Privacy Commissioner, *Complaint Case Notes and Complaint Determinations* <www.privacy.gov.au/act/casenotes/index.html> at 16 August 2006.

184 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 42. See also Rec 37.

185 Ibid, 139.

186 See, eg, Ibid, 130–131.

Question 6–16 Are the Privacy Commissioner's powers under the *Privacy Act* to make determinations appropriate and administered effectively?

Enforcement and review of determinations

6.131 The *Privacy Act* contains provisions for enforcement of determinations made under s 52 or, more specifically, of declarations made in determinations. The enforcement provisions only apply where a determination is made: by definition, they do not apply where the Commissioner has not made a determination, because there is nothing to enforce.

6.132 The Australian Consumers' Association submitted to the OPC Review that a wider power of enforcement should be conferred on the Commissioner. The Association's view was that the Commissioner should 'be able to enforce any directions given in relation to findings after an own motion investigation', thus ensuring that 'light handed' measures taken by the Commissioner have the 'weight of possible further action attached to them'.[187]

Enforcement of determinations against organisations

6.133 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.[188] The Commissioner lacks power to enforce the obligations directly. However, the obligations are enforceable in the Federal Magistrates Court or the Federal Court in proceedings commenced by the complainant, the Commissioner, or an adjudicator for the approved privacy code under which the determination was made.[189]

6.134 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'[190]—a relatively wide power of enforcement.

6.135 The court is to deal with the question of whether the respondent has engaged in conduct that constitutes an interference with the privacy of an individual by way of a hearing de novo.[191] The court may receive specified items of evidence, including a copy of the reasons for a determination made by a Commissioner or adjudicator, as

187 Ibid, 145.
188 *Privacy Act 1988* (Cth) s 55.
189 Ibid s 55A(1).
190 Ibid s 55A(2).
191 Ibid s 55A(5).

applicable, and any document that was before the Commissioner or adjudicator.[192] Pending the hearing, the court may grant an interim injunction.[193]

Enforcement of determinations against agencies

6.136 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.[194] 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 attention of the relevant members, officers and employees of the agency and that those relevant members, officers and employees desist from or perform conduct covered by the declaration.[195]

6.137 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.[196] This provision does not apply to organisations because of the limitations on Commonwealth judicial power. An application can be made to the Administrative Appeals Tribunal (AAT) for review of a decision by the Commissioner to include—or not include—a declaration for compensation or reimbursement.[197]

6.138 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 the Federal Magistrates Court for an order directing the agency or principal executive to comply.[198] The court may make 'such other orders as it thinks fit with a view to securing compliance by the respondent'.[199]

Merits review and judicial review

6.139 The OPC Review noted that there is no right of appeal to the AAT in respect of determinations about private sector organisations.[200] Stakeholders have expressed the view that the narrowness of the merits review available under the *Privacy Act* is one

---

192 Ibid s 55A(6)–(7). See also s 55B. In conducting a hearing and making an order under s 55A the court is to have regard to the matters in s 29(a): Ibid s 55A(7A).
193 Ibid s 55A(3)–(4).
194 Ibid s 58.
195 Ibid s 59.
196 Ibid s 60.
197 Ibid s 61(1). See also s 61(2).
198 Ibid s 62.
199 Ibid, s 62(4). See also s 61(5) regarding timing of the application.
200 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 129.

factor that prevents there being a useful legal jurisprudence of the Act on which people can rely.[201] Some stakeholders suggested that both the complainant and the respondent to a privacy complaint should have a right to seek merits review of determinations.[202]

6.140 A contrast is drawn with the position under New South Wales privacy legislation. In New South Wales, an applicant who is aggrieved by the conduct of a 'public sector agency'[203] is entitled to an internal review of that conduct by the agency concerned.[204] In this context, 'conduct' means the contravention by a public sector agency of an information protection principle or privacy code of practice that applies to the agency, or the disclosure by a public sector agency of personal information kept in a public register.[205] If the person who applied for internal review is not satisfied with the findings of that review or the action taken by the public sector agency, the person may apply to the Administrative Decisions Tribunal for review of the conduct that was the subject of the original application for internal review.[206] On reviewing the conduct of the public sector agency concerned, the Tribunal may decide not to take any action on the matter or it may decide to make one or more orders, including an order requiring the public sector agency to pay compensatory damages of up to $40,000.[207] A party can appeal an order or decision of the Tribunal to the Appeal Panel of the Tribunal.[208]

Question 6–17 Are the *Privacy Act* provisions for enforcing determinations adequate and administered effectively?

Public interest determinations

6.141 The Commissioner can make a public interest determination about the acts and practices of an agency or organisation. In essence, a public interest determination is a determination by the Commissioner that an act or practice of an agency or organisation which would otherwise breach an IPP, NPP or approved privacy code should be disregarded for the purposes of s 16 (which requires agencies to comply with the IPPs) or s 16A (which requires organisations to comply with approved privacy codes or the NPPs) while the determination is in force.[209] A public interest determination, therefore,

---

201 Ibid, 137–138.
202 Ibid, 138–139, 144 and Rec 40. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.
203 Public sector agency is defined in s 3 of *Privacy and Personal Information Protection Act 1998* (NSW).
204 Ibid s 53.
205 Ibid s 52(1). Note that a reference to conduct also includes a reference to alleged conduct: s 52(2).
206 Ibid s 55(1).
207 Ibid s 55(2).
208 Ibid s 56. See also Acting NSW Privacy Commissioner, *Consultation PC 8*, Sydney, 9 March 2006.
209 *Privacy Act 1988* (Cth) s 72. As at 15 August 2006, there were nine public interest determinations registered, dated from September 1989 with the most recent determination dated October 2002. One temporary public interest determination is current (effective from 10 February 2006 to 22 December 2006); Office of the Privacy Commissioner, *Public Interest Determinations* <www.privacy.gov.au/act/publicinterest/index.html> at 27 August 2006.

relieves an agency or organisation from its obligations regarding individuals' privacy under the *Privacy Act*.

Nature of determinations

6.142 A public interest determination 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.[210]

6.143 A public interest determination made by the Commissioner in relation to organisations, but not agencies, can be given general effect. Thus, the Commissioner may make a public interest determination that no organisation is taken to contravene s 16A if, while that determination is in force, an organisation does an act, or engages in a practice, that is the subject of a determination in relation to that organisation or any other organisation.[211]

Temporary public interest determinations

6.144 The Commissioner also has the power to issue a temporary public interest determination. A temporary public interest determination has the same effect as a public interest determination but is limited in duration to a maximum of 12 months.[212]

6.145 The Commissioner can make a temporary public interest determination in relation to an act or practice of an agency or organisation that is the subject of an application for a public interest determination where the application raises issues that require an urgent decision.[213] The Commissioner can give a temporary public interest determination in respect of an act or practice of an organisation general effect, so that it applies to other organisations.[214]

6.146 It is important to note, however, that the Commissioner cannot make a temporary public interest determination, for example in response to an emergency,[215] without an application having been made for a public interest determination.

---

210 *Privacy Act 1988* (Cth) s 72(1)–(2). Emphasis added.
211 Ibid s 72(4).
212 Ibid ss 80A(3)(a), 80B.
213 Ibid s 80A(1).
214 Ibid s 80B(3)–(4).
215 This issue and the possibility of using a temporary public interest determination to declare an emergency, is discussed in Ch 4. As noted in that chapter, the Australian Government introduced the Privacy Legislation Amendment (Emergencies and Disasters) Bill 2006 into Parliament on 13 September 2006. The Bill makes special provision for the collection, use and disclosure of personal information in emergencies and disasters.

Question 6–18 Are the Privacy Commissioner's powers under the *Privacy Act* to make public interest determinations, including temporary public interest determinations, appropriate and administered effectively?

Injunctions

6.147 In addition to powers to grant an interim injunction in certain instances, the *Privacy Act* contains wider provisions regarding injunctions. In particular, s 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.[216]

6.148 Two features of the injunctions power are significant. First, it does not only concern enforcement of determinations. It is a freestanding provision which deals with contraventions of the *Privacy Act*. Secondly, the 'standing' requirement is wide—the application may be made by the Commissioner 'or any other person'.[217]

6.149 Broadly speaking, s 98 establishes a position quite distinct from the general law on injunctions. For instance, it provides that 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.[218] 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.[219]

6.150 There appears 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.[220] The Commissioner has noted that it would only seek an injunction 'when other more informal means have failed to yield a satisfactory outcome'.[221] It is not clear why other persons have rarely sought an injunction. One possible reason may be that the procedures involved in obtaining an injunction are of a

---

216 *Privacy Act 1988* (Cth) s 98(1). See s 98(2).

217 *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* (2004) 148 FCR 145, [40]. See also [55].

218 *Privacy Act 1988* (Cth) s 98(5)(b). See also s 98(6).

219 Ibid s 98(7).

220 The OPC Review noted that to its knowledge the injunction power has been only used once, in *Seven Network (Operations) Ltd v Media Entertainment and Arts Alliance* (2004) 148 FCR 145—see Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 126 fn 90.

221 Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001), 3.

degree of formality and expense that make that approach undesirable. The ALRC is interested in views on this issue.

Question 6–19 Are the *Privacy Act* provisions for obtaining injunctions adequate and effective?

Powers relating to privacy codes

Effect of codes

6.151 Organisations may be bound by an approved privacy code rather than the NPPs. A code applies to the exclusion of the NPPs, subject to the provisions on TFNs and credit reporting (Part IIIA).[222]

6.152 The Revised Explanatory Memorandum to the Privacy Amendment (Private Sector) Bill 2000 stated that the proposed scheme for approved privacy codes had several advantages:

> First, it would ensure that all organisations would be required to adopt fair practices in relation to handling personal information, that there would be an identifiable mechanism for making a complaint about any organisation, and consistency and transparency in the remedies available to the consumer. Second, it would allow industries to develop codes tailored to the specific requirements of that industry. This would allow flexibility and sensitivity to industry and market needs. Third, industry would retain ownership of its code and its implementation process. Fourth, codes could be written in language readily understood by the operators in the industry, thus allowing their direct use at the operational level. Finally, the possibility of being able to amend codes would ensure that changing circumstances could be readily accommodated.[223]

6.153 There are currently three codes listed on the Register of Approved Privacy Codes found on the OPC's website.[224] These 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 (which came into effect on 1 September 2006). There are also two code applications currently

---

222 *Privacy Act 1988* (Cth) s 16A. The code may also cover exempt acts or practices, in effect imposing enforceable privacy obligations on organisations in respect of matters that would otherwise fall outside the Act: s 18BAA.

223 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 19.

224 Office of the Privacy Commissioner, *Privacy Codes* <www.privacy.gov.au/business> at 16 August 2006. Note that there was a fourth code approved by the Privacy Commissioner—the *General Insurance Information Privacy Code*. This code was revoked on 30 April 2006.

being considered by the OPC, being the Australian Casino Association Privacy Code and the Internet Industry Privacy Code.

Approval and review of codes

6.154 The Commissioner's powers regarding privacy codes are generally to:

- approve privacy codes and variations of approved privacy codes and to revoke those approvals;[225]
- review the operation of approved privacy codes;[226]
- prepare and publish guidelines about development, approval and variation of privacy codes, and about complaint handling processes under codes;[227]
- 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;[228] and
- consider applications for review of determinations of adjudicators (other than where the Commissioner is the adjudicator) in relation to a complaint.[229]

6.155 The content of a code must meet set standards.[230] In particular, a 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'.[231] The NPPs are in some respects very detailed;[232] codes must accordingly meet an equivalent level of prescription.

6.156 Subscription to a code is to be voluntary.[233] Codes are to specify 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.[234]

Complaints under codes

6.157 The *Privacy Act* requires fair, impartial, open and responsible processes and actions in relation to complaints made under a code.[235] The procedures applying to

---

225 *Privacy Act 1988* (Cth) s 27(1)(aa).
226 Ibid s 27(1)(ad). Review occurs under s 18BH.
227 Ibid s 27(1)(ea).
228 Ibid s 27(1)(ac).
229 Ibid s 27(1)(ae). See also s 18BI.
230 This is imposed by Ibid s 18BB, through the requirement that the Commissioner may approve a privacy code if, and only if, he or she is satisfied of certain matters.
231 Ibid s 18BB(2)(a).
232 The NPPs are discussed in Ch 4.
233 *Privacy Act 1988* (Cth) s 18BB(2)(c).
234 Ibid ss 18BB(2)(b), 18BB(6)–(7).

code complaints (made to an adjudicator appointed under the code) are aligned with the procedures regulating complaints to the Commissioner under the NPPs and IPPs. Codes must also meet the Commissioner's guidelines, if any, in relation to making and dealing with complaints, and with prescribed standards.[236]

Previous inquiries

6.158 There were several issues raised in relation to the code provisions in the OPC Review and the Senate Committee privacy inquiry. These are discussed below.

Binding codes

6.159 Some stakeholders submitted to the OPC Review 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.[237] Support for this proposition was not universal.[238] As noted earlier, the OPC Review canvassed the possibility that problems to do with systemic issues could be addressed by giving the Commissioner power to issue binding guidelines, and that a power to impose a non-voluntary code was considered to be an alternative or additional remedy for systemic issues.

6.160 The OPC Review noted that the *Privacy Act* could be amended to provide for any of the following approaches.

- After identifying the need for a code in a specific sector, the Attorney-General could direct the Commissioner to develop a code in consultation with key stakeholders.
- The relevant Minister could be given power to declare a code mandatory for a particular industry, as currently occurs under the *Trade Practices Act 1974* (Cth).
- The Commissioner could make a binding code on his or her initiative, in consultation with key stakeholders.
- The Commissioner could be given the power to issue a binding industry standard where a particular industry fails to implement a self-regulatory code.[239]

---

235 Ibid s 18BB(3).
236 Ibid s 18BB(3)(a).
237 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 145.
238 Ibid, 145.
239 Ibid, 46–47. Not all of these approaches require legislative change.

6.161 The OPC Review recommended that the Australian Government should consider amending the *Privacy Act* to give the Commissioner power to make binding codes.[240] A situation where the OPC Review thought such a power would be useful is in relation to tenancy databases, where 'in practice, the impact of the Commissioner's determinations … appears to have been limited'.[241]

Low take-up of codes

6.162 Codes have been little used since the code provisions were introduced in 2000. The OPC Review concluded that the privacy code provisions are an area 'where the objectives of the private sector provisions have not been achieved in the way that was anticipated'.[242] The OPC Review noted, however, that there was no call for the repeal of the code provisions despite the very low level of take-up, and that 'most businesses appear content to be regulated by the NPPs and to have the Office as their external complaints handling body'.[243]

6.163 Stakeholders also expressed concern in the Senate Committee privacy inquiry about codes that applied horizontally (ie, to a technology) rather than vertically (ie, to industries or organisations).[244] The concern was that a code that applied to a particular technology (eg, biometrics) may only cover part of an organisation's activities, and any activities that did not involve the use of the technology would then be subject to the NPPs or another code.[245] This could make it difficult for organisations to know and understand their privacy obligations.

Question 6–20 Are the *Privacy Act* provisions for approving privacy codes appropriate and effective? Are privacy codes an appropriate method of regulating and complying with the Act? Why have privacy codes been so little used? Should the Privacy Commissioner have the power, on his or her initiative, to develop and impose a binding code on organisations or agencies?

Compliance models

6.164 The discussion so far has set out the various powers of the OPC, and in particular, the ways in which the Commissioner promotes compliance with the *Privacy Act*. This section will consider more broadly the compliance model underpinning the *Privacy Act*, being the specific modes for fostering and enforcing compliance,

240 Ibid, Rec 7.
241 Ibid, 159.
242 Ibid, 3.
243 Ibid, 3.
244 See Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.91]–[3.93].
245 See Ibid, [3.90].

including the statutory provisions and the manner of their administration and enforcement.

6.165 Stakeholders in the OPC Review were divided as to whether the Commissioner has sufficient powers under the *Privacy Act*. On the one hand, organisations and business groups generally found that the existing provisions provided appropriate rights and the powers in the *Privacy Act* were sufficient.[246] For instance, it was suggested that the existing enforcement powers including those relating to determinations were a 'powerful enough incentive for organisations to comply'.[247] Stakeholders from business groups submitted that the right balance had been achieved. They also supported the Commissioner's approach to compliance (ie, its limited use of formal enforcement powers and its focus on cooperative resolution of issues) and submitted that it should continue.[248]

6.166 In contrast, consumer and advocacy groups expressed strong concern about the lack of enforcement mechanisms in the *Privacy Act*, particularly in relation to determination enforcement.[249] Stakeholders from these groups also submitted that the Commissioner's approach to compliance was ineffective[250] and that the Commissioner does not use his or her existing powers effectively (eg, the limited use of the power to make determinations).[251]

6.167 The Senate Committee privacy inquiry also acknowledged in its recommendations the views of stakeholders about the inadequate powers of the OPC.[252] For instance, the Senate Committee received submissions that the powers of the OPC are 'too restricted'[253] and 'relatively weak'[254] and that in comparison with European Union jurisdictions the enforcement powers and procedures under the Australian regime 'engender a more subtle approach to breaches'.[255] It was also suggested that the *Privacy Act* itself imposed only a '"bare bones" privacy framework with, for example, no required reporting and no real capacity for the OPC to impose direct cost on industry'.[256]

---

246 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 130–131.
247 Ibid, 131.
248 Ibid, 130–131.
249 Ibid, 133.
250 Ibid, 131–133.
251 Ibid, 134–135.
252 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.53].
253 Ibid, [6.35].
254 Ibid, [6.40].
255 Ibid, [6.41].
256 Ibid, [6.25].

6.168 The Senate Committee privacy inquiry heard criticism of the determinations provisions on the ground that enforceable steps to remedy an infringement can only be obtained if the Commissioner or the complainant takes the further step of bringing an action in the Federal Court or the Federal Magistrates Court. It was pointed out that the Australian Broadcasting Authority, by contrast, has certain powers to make binding, enforceable determinations—non-compliance with which is an offence.[257]

6.169 Drawing on these inquiries, there are two questions to be addressed. First, does the *Privacy Act* contain sufficient powers to ensure compliance by agencies and organisations? Secondly, does the *Privacy Act* contain sufficient penalties and remedies in the event of non-compliance?

Powers to ensure compliance

6.170 As a general observation, the *Privacy Act* takes a 'light-touch' approach to compliance, particularly in the private sector provisions.[258] As the OPC Review points out, the Commissioner's powers to audit agencies, credit providers, credit reporting agencies and TFN recipients are not replicated in the private sector provisions, and the Commissioner cannot report to Parliament about the failure of an organisation to respond to any recommendations following an own-motion investigation.[259]

6.171 The OPC's approach to compliance places emphasis on providing advice, assistance and information.[260] The OPC has issued only eight determinations since the *Privacy Act* came into operation and has never taken the step of enforcing a determination or seeking an injunction in the Federal Court or Federal Magistrates Court.

6.172 The OPC Review acknowledged the concern expressed by some consumers and advocates that the enforcement of the *Privacy Act* is 'soft'[261] and 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 making power.[262] As set out above, some submissions to the Senate Committee privacy inquiry also expressed the view that the Commissioner's powers are inadequate.[263]

---

257 Ibid, [6.40], referring to *Broadcasting Services Act 1992* (Cth) sch 5.

258 See for example Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 128.

259 Ibid, 128.

260 Ibid, 125–126. 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).

261 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 152.

262 Ibid, Rec 37. See also Rec 42.

263 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.35]–[6.40].

6.173 In asking whether there are sufficient powers to ensure compliance with the *Privacy Act*, the Inquiry must consider whether there should be more obligations placed on organisations and agencies to illustrate active compliance with the Act, and whether there should be more powers and functions invested in the Commissioner to ensure compliance.

Further obligations on agencies and organisations

6.174 The OPC Review noted that a 'number of submissions put the view that at present, the *Privacy Act* does not provide sufficient powers to ensure that businesses are aware of their obligations to protect privacy, or know how to implement them in practice and carry through on implementation'.[264] Some suggestions about further obligations on agencies and organisations made to the OPC Review, the Senate Committee privacy inquiry or the ALRC have included:

- extending the Commissioner's audit powers to the private sector;
- introducing self-auditing and reporting requirements;
- requiring organisations to make available an approved internal dispute resolution process;[265]
- requiring organisations when collecting information to inform individuals of their ability to make a complaint about a privacy issue;[266]
- requiring the preparation of privacy impact assessments in more situations;[267]
- requiring mandatory reporting of privacy breaches.[268]

---

264 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 135.

265 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.24], [6.37].

266 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 160 and Rec 41. See also Ch 4.

267 Ibid, 256; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 5; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; N Waters, *Consultation PC 17*, Sydney, 2 May 2006. See also G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

268 See Question 4–35 and Question 11–3(d). See also N Miller, 'Data Leaks Under Review', *The Sydney Morning Herald* (Sydney), 8 August 2006, 27; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006 and M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006.

Further powers for the Commissioner

6.175 If further obligations were to be placed on organisations and agencies, it is likely that related functions and powers to oversee those obligations would need to be placed on the Commissioner. In addition, it may be appropriate to expand the powers of the Commissioner to ensure compliance. For example the Commissioner could be given power to serve a compliance notice in the event of serious or repeated breaches of the *Privacy Act*.[269] In order to address concerns about the lack of transparency in the complaints process,[270] the Commissioner could be required to publish online a comprehensive manual of its complaint resolution policies and procedures.[271]

Remedies and penalties to ensure compliance

6.176 The second issue raised above is whether the *Privacy Act* contains sufficient penalties and remedies in the event of non-compliance with the Act. Regulatory theorists have suggested that the ideal regulatory approach is the 'enforcement pyramid', by which regulators use coercive sanctions only when less interventionist measures have failed to produce compliance.[272] Under this model, 'breaches of increasing seriousness are dealt with by sanctions of increasing severity, with the ultimate sanctions … held in reserve as a threat'.[273]

6.177 The VLRC considered a sanctions pyramid in its *Workplace Privacy: Final Report*.[274] It noted that a sanctions pyramid approach 'relies initially on encouraging conforming behaviour through information and education about legislative requirements'.[275] In the case of minor breaches, the regulator will usually warn non-compliers and give them an opportunity to remedy the problem, before any penalty is imposed.[276] However, if the breach is serious or repeated, or arises out of a systemic issue, it said that more severe penalties should be imposed because 'persuasive and compliance-oriented enforcement methods are more likely to work where they are backed up by the possibility of more severe methods'.[277]

---

269 For instance the Northern Territory Information Commissioner has the power to serve a compliance notice—see *Information Act 2002* (NT) s 82. See also Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.91]–[4.93].

270 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. See also Rec 42.

271 Ibid, 142. See also Rec 43.

272 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [3.32].

273 Ibid, [3.33].

274 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.75]–[4.80].

275 Ibid, [4.76].

276 Ibid, [4.76].

277 Ibid, [4.77] citing C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 529.

Application of enforcement pyramid to the Privacy Act

6.178 In some respects the *Privacy Act* adopts a pyramid-type structure for enforcing compliance. Consistent with the enforcement pyramid model, the approach relies initially on encouraging compliance, with the determinations (and enforcement in the courts) and injunctions held in reserve.

6.179 While there is some degree of escalation involved in these remedies, the Commissioner does not possess many powers to impose penalties on transgressors without going through the courts. In contrast, other schemes, such as the workplace privacy scheme proposed by the VLRC and the *Information Act 2002* (NT), contain stronger penalties, including monetary penalties and compliance notices.

Administrative penalties

6.180 The ALRC has previously defined administrative penalties as 'sanctions imposed by the regulator, or by the regulator's enforcement of legislation, without intervention by a court or tribunal'.[278] The ALRC has suggested that true administrative penalties are automatic, non-discretionary monetary administrative penalties.[279]

6.181 Most administrative penalties are imposed for failure to meet certain requirements, such as not lodging a document on time or failing to comply with miscellaneous obligations, such as keeping proper records.

6.182 The ALRC is interested in views on whether administrative penalties should be attached to some obligations of agencies and organisations under the *Privacy Act*, and if so, what type of administrative penalties and in which circumstances they should be imposed.

Enforceable undertakings

6.183 Enforceable undertakings are a relatively recent enforcement response and are currently used by the Australian Competition and Consumer Commission (ACCC) and ASIC. 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.[280]

---

278 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.64].
279 Ibid, [2.70].
280 Ibid, [2.159].

6.184 The ACCC is able to accept enforceable undertakings under s 87B of the *Trade Practices Act 1974* (Cth) (TPA). If the ACCC considers that the person who gave the undertaking has breached any of its terms, the ACCC can apply to the court for an order directing the person to comply with that term of the undertaking.[281]

6.185 The ACCC has stated that it 'regards s 87B as an important compliance tool for use in situations where there is evidence of a breach or potential breach of the [TPA] that might otherwise justify litigation'.[282] It has said that in negotiating s 87B undertakings the ACCC's broad objectives are:

- cessation of the conduct leading to the alleged breach;
- redress for parties adversely affected by the conduct;
- implementation of compliance measures to help prevent future breaches by the business concerned; and
- by means of publicity, an educative and deterrent effect in the community at large and in particular in the industry concerned.[283]

6.186 The ALRC is interested in views about whether the Commissioner should have a power to accept an enforceable undertaking where he or she believes a breach of the *Privacy Act* has occurred or may occur.[284] For instance, an enforceable undertaking may be one way of dealing with systemic or serious breaches of the *Privacy Act* and the Commissioner could adopt similar objectives to those outlined by the ACCC in negotiating enforceable undertakings.

Publicity

6.187 Publicity can be a penalty.[285] In particular, publicity can operate as a formal, legislated sanction or it can operate as a negative perception of an agency or organisation which arises by virtue of the imposition of another penalty on the agency or organisation.

6.188 An example of publicity as a penalty in its own right is the ACCC's power to apply to the court to make an 'adverse publicity order' in relation to a person who has been ordered to pay a pecuniary penalty under the TPA, or who is guilty of an offence under certain parts of the TPA.[286] As noted earlier, the Commissioner does not have

---

281 *Trade Practices Act 1974* (Cth) s 87B. Other orders are also available.

282 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), 1.

283 Ibid, 3.

284 This was a suggestion made 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), 145–146.

285 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.138].

286 *Trade Practices Act 1974* (Cth) s 86D. Note that ASIC is also empowered to apply for an adverse publicity order under s 12GLB of the *Australian Securities and Investments Commission Act 2001* (Cth).

power to report directly to Parliament or to table a report in relation to complaint made about an act or practice of an organisation, or which is referred to the Commissioner by a code adjudicator.[287]

6.189 Informal publicity or publicity arising from another penalty can still have serious 'penalising' characteristics. For instance, the OPC has previously recognised that:

> On occasion there may be some merit in making public the circumstances of a particular complaint or investigation. This may be, for example, where there is already publicity around a particular matter before it reaches the Office or where, despite all the other approaches the Office has taken, an organisation continues to engage in behaviour that constitutes an interference with privacy. This would clearly be a serious step which could have commercial consequences for the organisation concerned. It would only be appropriate in rare circumstances.[288]

6.190 The OPC has issued media statements outlining the actions taken in respect of particular organisations and agencies.[289] The OPC's usual practice is to de-identify parties to a complaint in any case notes it publishes. However, it does not de-identify parties to a determination and, in light of the OPC's practice of publishing determinations on its website, there is an element of informal publicity (or 'naming and shaming') involved in that process.[290]

6.191 The use of informal publicity could be attached to any proposed obligation to report privacy breaches. For example, as part of the reporting process, the OPC could have the power to issue a press release advising of receipt of the report from the agency or organisation.[291] It could also be used in connection with enforceable undertakings, such as by requiring the Commissioner to issue press releases when he or she accepts an undertaking and to maintain a public register of undertakings on his or her website.

6.192 The use of publicity as a penalty was raised in a consultation with the ALRC. In particular, one stakeholder expressed the view that adverse publicity is one of the most

---

287 See *Privacy Act 1988* (Cth) s 30(6).

288 Office of the Federal Privacy Commissioner, *The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act 1988*, Information Sheet 13 (2001), 3.

289 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).

290 See Office of the Privacy Commissioner, *Complaint Case Notes and Complaint Determinations* <www.privacy.gov.au/act/casenotes/index.html> at 16 August 2006.

291 This could take a similar form to the requirement that the Commissioner publish notice of the receipt by the Commissioner of an application for a public interest determination under *Privacy Act 1988* (Cth) s 74(1).

potent weapons to ensure an organisation's compliance.[292] The ALRC is interested in views in relation to formal and informal publicity orders.

Remedies in the nature of damages

6.193 There is currently no allowance for direct civil action by individuals against agencies or organisations that breach the *Privacy Act*.[293] The only compensation available to complainants is through the Commissioner's power to make a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint.[294] This can only be enforced against Commonwealth agencies and principal executives (not organisations) because of the limitations on Commonwealth judicial power. 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.[295]

6.194 One stakeholder submitted to the Senate Committee privacy inquiry that direct civil actions should be allowed if the OPC Review's recommendation that the Australian Government amend the *Privacy Act* to give the Commissioner a further discretion not to investigate complaints is implemented.[296] The ALRC is interested in views on this suggestion and more broadly as to whether individuals should have access to a direct civil action against agencies or organisations that breach the *Privacy Act*.

Infringement notices

6.195 Infringement notices (sometimes called a penalty notice) are administrative methods of dealing with certain breaches of the law. They are not a true administrative penalty, but rather

> an administrative device to dispose of a matter that involves a criminal or non-criminal breach. When such a breach is committed, the relevant agency may prosecute or take civil penalty proceedings, or may issue an infringement notice offering the

---

292 M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006.

293 The related question of whether a cause of action for breach of privacy should be recognised by the courts or the legislature in Australia is discussed in Ch 1. Also note that an individual can seek an injunction under *Privacy Act 1988* (Cth) s 98, as discussed above.

294 Ibid s 52(1)(b)(iii).

295 *Trade Practices Act 1974* (Cth) s 82.

296 See Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [6.30]. The 'further discretion' is not to investigate a complaint where the harm to individuals is minimal and there is no public interest in pursuing the matter: 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.

> offending party the chance to discharge or expiate the breach through payment of a specified amount.[297]

6.196 Infringement notices are typically used for low-level offences and where a high volume of uncontested contraventions is likely, such as traffic and parking violations.[298]

6.197 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.[299]

6.198 The *Corporations Act 2001* (Cth) provides for a penalty notice procedure for less serious breaches of the Act. In particular, where ASIC has reason to believe that a person has committed a 'prescribed offence',[300] it may issue that person with a notice alleging that an offence has been committed, setting out the prescribed particulars of the offence, and stating that if the person pays the amount specified in the notice and (where applicable) rectifies an omission within 21 days of the issue of the notice, ASIC will not take further action.[301]

6.199 The ALRC is interested in views as to whether an infringement notice scheme may be useful in addressing breaches of the *Privacy Act*, and in what circumstances it should be imposed.

Civil pecuniary penalties

6.200 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.[302] The TPA and *Corporations Act* contain civil penalty regimes.

---

297 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.67].

298 Ibid, [2.130].

299 Ibid, [2.130].

300 'Prescribed offence' is defined in *Corporations Act 2001* (Cth) s 1313(8).

301 Ibid s 1313. See also Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [12.20].

302 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.107].

6.201 A stakeholder in the OPC Review said it is hard to convince some company boards to comply with privacy laws when no schedule of penalties is attached to the NPPs.[303] This view was also raised in consultations with the ALRC in this Inquiry.[304]

6.202 One possibility is to amend the *Privacy Act* so that certain provisions are defined as civil penalty provisions. The Commissioner could then apply to the Federal Court or Federal Magistrates Court for a declaration that a person has contravened a civil penalty provision. If the court is satisfied that the person has contravened a civil penalty provision it may order the agency or organisation to pay a pecuniary penalty.

6.203 The ALRC is interested in views on whether there should be a civil penalty regime in the *Privacy Act*, and if so, what breaches should be liable to pecuniary penalties. For example, would it be appropriate to nominate ss 16 and 16A, which respectively prohibit an agency or organisation from doing an act or engaging in a practice that breaches an IPP or NPP, as civil penalty provisions? One stakeholder expressed the view to the ALRC that civil penalties could attach to non-compliance with any proposed self-auditing and reporting requirements.[305] The VLRC in its proposed legislation recommended attaching civil penalties to non-compliance with a compliance notice.[306]

Criminal penalties

6.204 The *Privacy Act* does contain some criminal offences. For instance, furnishing information knowing that is false or misleading in a material particular is an offence carrying a penalty of $2,000 or 12 months imprisonment, or both.[307] 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.[308]

6.205 The ALRC is interested in views on whether there should be criminal penalties attached to specific contraventions of the *Privacy Act*, and if so, in what circumstances. For instance, would it be appropriate for criminal penalties (such as a fine) to attach to non-compliance with any proposed compliance notice issued by the Commissioner

---

303 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 133. Note it is unclear whether 'penalties' relates to criminal or civil penalties (or both).

304 See Office of the Privacy Commissioner and Acting NSW Privacy Commissioner, *Consultation PM 9*, Sydney, 24 July 2006; Law Council of Australia Privacy Working Group, *Consultation PC 32*, Sydney, 12 July 2006; A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

305 M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006.

306 See Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), [4.91].

307 *Privacy Act 1988* (Cth) s 65(3).

308 Ibid s 18K(4).

(instead of, or in addition to, civil penalties) or to a reckless, intentionally dishonest or flagrant contravention of the *Privacy Act*?[309]

Resourcing implications

6.206 Many possible reforms of the *Privacy Act* canvassed in relation to the powers and functions of the OPC potentially have resourcing implications. The issue of adequate funding was raised in both the OPC Review and the Senate Committee privacy inquiry, with both inquiries recommending that the OPC be adequately resourced.[310]

Question 6–21 Is the current compliance model used in the *Privacy Act* appropriate and effective to achieve the Act's purposes? If not, is that because of its content, its administration, or some other reason?

Question 6–22 Does the range of remedies available to enforce rights and obligations created by the *Privacy Act* require expansion? For example, should the available remedies include any or all of the following for particular breaches of the Act:

(a) administrative penalties;

(b) enforceable undertakings or other coercive orders;

309 For example, it is an offence under the *Corporations Act 2001* (Cth) s 84 if a director is reckless or intentionally dishonest and fails to exercise his or her powers and discharge his or her duties in good faith in the best interest of the corporation or for a proper purpose. In addition, the UK Department of Constitutional Affairs has announced its intention to add jail terms to the sentencing regime under the *Data Protection Act 1998* (UK), together with unlimited fines. See S Hills, 'Insurance Industry Warned of Data Abuse Prison Threat', *Insurance Age*, 1 September 2006, 43 and United Kingdom Government Information Commissioner's Office, *What Price Privacy? The Unlawful Trade in Confidential Personal Information* (2006).

310 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 45; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [7.54] and Rec 19.

(c) remedies in the nature of damages;

(d) infringement notices;

(e) civil penalties;

(f) criminal sanctions?

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation

Contents

Introduction

7.1 This chapter 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. Issues related to inconsistency and fragmentation are also considered in other chapters. The inconsistencies between the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) are

considered in Chapter 4, the fragmentation that results from the various exemptions under the *Privacy Act* is outlined in Chapter 5, inconsistency and fragmentation in the regulation of health information is discussed in Chapter 8, the interaction of the *Privacy Act* and telecommunications legislation is considered in Chapter 10, and regulatory gaps resulting from the use of new technologies are outlined in Chapter 11.

7.2 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 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* (Senate Committee privacy inquiry) heard that:

> what is emerging is a patchwork of privacy protection, driven in various ways by divisions between public and private sectors of the economy, state and federal levels of government, specific economic sectors (such as health), emerging technologies all of which have subverted the aim of the legislation in this regard. Not least of the drivers for these divisions are the gaps embodied in the federal legislation (such as the small business exemption and employee record exception) that was intended to deliver the nationally consistent scheme.[4]

7.3 It has been observed that inconsistency in the regulation of personal information stems largely from the failure of federal law to cover the field. For example, the Office of the Privacy Commissioner (OPC) has suggested that the exemptions under the *Privacy Act* may be undermining national consistency by leading some states and territories to develop their own laws.[5] The Australian Privacy Foundation (APF) has noted that

---

1 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1092].

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 and 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 and 4.48.

3 Inconsistency in the regulation of personal information has been raised as an issue in consultation meetings with the ALRC: A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006; G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006; R Magnusson, *Consultation PC 1*, Sydney, 25 February 2006; Australian Privacy Foundation, *Consultation PC 4*, Sydney, 27 February 2006; D Giles, *Consultation PC 6*, Sydney, 2 March 2006; NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006; B Bainbridge, *Consultation PC 12*, Canberra, 30 March 2006; G Hill, *Consultation PC 21*, Melbourne, 8 May 2006; Commonwealth Ombudsman, *Consultation PC 11*, Canberra, 30 March 2006; M Jackson, *Consultation PC 27*, Melbourne, 10 May 2006.

4 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.20].

5 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 45; Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.22]. Exemptions are discussed in detail in Ch 5.

> it is hardly surprising that, faced with major gaps and weaknesses, the States and Territories have felt it necessary to provide their citizens with additional protection both in general privacy laws and in specific areas of health privacy and surveillance.[6]

7.4 A threshold issue is whether national consistency should be one of the goals of the regulation of personal information. Even if national consistency is a desirable goal, there may be some circumstances where inconsistency is justified. For example, particular industry sectors may require more or less stringent laws to regulate the management of personal information. Chapter 2 considers various models for dealing with inconsistency and fragmentation in the regulation of personal information.

Problems caused by inconsistency and fragmentation

7.5 A number of problems caused by inconsistency and fragmentation are raised throughout this chapter, including complexity of privacy regulation, varying levels of privacy protection, and regulatory gaps. This section of the chapter discusses some specific problems caused by inconsistency in privacy regulation including an increase in compliance burden and cost and the impeding of national initiatives and information sharing. The difficulties experienced by government contractors and national companies are also considered.

Compliance burden and cost

7.6 The Terms of Reference for the current 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.[7] 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.[8]

7.7 The Taskforce on Reducing Regulatory Burdens on Business heard that inconsistency in the areas of workplace surveillance, direct marketing and telemarketing laws, and having to supply information to multiple government agencies, contributed to compliance burdens and costs.[9] 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

---

6 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.21].

7 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.

8 Australian Chamber of Commerce and Industry, *Submission to the Taskforce on Reducing Regulatory Burdens on Business*, 1 November 2005, 5.

9 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.

federal privacy laws (including the *Privacy Act* and the *Telecommunications Act 1997* (Cth)) contributes to compliance costs.[10]

7.8 The ALRC has heard similar comments in the current Inquiry.[11] The ALRC was told that the proliferation and fragmentation of privacy laws at the federal, state and territory levels significantly increases compliance burden and cost. One stakeholder reported that state entities can find it difficult to determine whether privacy legislation applies to them.[12] The ALRC also heard that health organisations may be required to comply with six layers of privacy regulation.[13] Additionally, the ALRC was told that if a Victorian charity that provides a health service receives funding from both state and federal governments it may need to deal with the NPPs and the IPPs, as well as Information Privacy Principles and Health Privacy Principles under state legislation.[14]

7.9 However, the Senate Committee privacy inquiry heard conflicting views in relation to compliance burden and cost.[15] 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.[16] Other submissions argued, however, that the benefits of privacy regulation to business and Australian society outweigh the costs of compliance.[17] 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.[18]

7.10 The Taskforce on Reducing Regulatory Burdens on Business noted that achieving nationally consistent privacy laws is an important factor in reducing compliance costs for business.[19] The 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.[20] In its response to this recommendation the Australian Government stated that:

---

10 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.
11 Federal Privacy Commissioner, *Consultation PM 1*, Sydney, 6 December 2005; D Mico, *Consultation PC 9*, Sydney, 14 March 2006.
12 G Hill, *Consultation PC 21*, Melbourne, 8 May 2006.
13 R Magnusson, *Consultation PC 1*, Sydney, 25 February 2006.
14 M Richardson and K Clark, *Consultation PC 24*, Melbourne, 9 May 2006.
15 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.149]–[4.154].
16 Ibid, [4.152].
17 Ibid, [4.150].
18 Ibid, [4.149]–[4.154].
19 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].
20 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.[21]

7.11 The ALRC is interested in hearing from organisations and agencies about whether privacy regulation contributes to an unjustified compliance burden or cost. In particular, the ALRC would be interested in receiving information that can quantify the compliance burden experienced due to problems associated with privacy regulation.

National organisations

7.12 As outlined below, there are a number of significant differences between privacy regimes in each Australian state and territory. The ALRC is interested in hearing what issues this raises for organisations that operate in more than one Australian state or territory. In ALRC 22, the ALRC noted that:

> Especially where controls on handling computerised information are concerned there are good reasons why uniformity with the States and the Northern Territory is desirable. Information handling, for example in banking, insurance and government administration, is now a national industry and is conducted as such. Uniformity is therefore desirable to ensure the smooth functioning of the industry, especially as a great deal of information now crosses State borders.[22]

7.13 Inconsistency and fragmentation in privacy regulation continue to be 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.[23]

7.14 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 jurisdiction).[24] The Taskforce on Reducing Regulatory Burdens on Business also noted that this was an issue in the context of different laws relating to direct marketing.[25]

---

21 Australian Government, *Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business—Australian Government's Response* (2006), 26.

22 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1088].

23 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 40.

24 Ibid, 66.

25 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.

National initiatives

7.15 Inconsistency and fragmentation in privacy regulation can also be a barrier to national initiatives. Inconsistencies between federal, state and territory privacy laws can unnecessarily complicate the implementation of programs and services at a national level. For example, the ALRC has been told that it is not desirable to have a national e-health system that is reliant on a patchwork regulatory scheme such as the current privacy scheme.[26] The OPC has noted in relation to a national e-health system that:

> as well as having a national standard for protecting the handling of health information (that is, a consistently enacted National Health Privacy Code), there appears to be a need for specific enabling legislation for electronic health records systems generally. This is the case particularly for an overarching national (or enabling) system, such as Health*Connect*.[27]

Multiple regulators

7.16 Some industries are required to comply with multiple layers of privacy regulation which is overseen by more than one regulator. This has been identified as an issue in the telecommunications industry[28] 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.[29]

7.17 The ALRC has also heard, however, that industry ombudsmen and the OPC have taken opposing views in relation to the same privacy complaint.[30] The OPC Review was told that there is no clear jurisdiction in relation to privacy complaints between the federal and New South Wales privacy commissioners.[31] Consumers may not know which regulator to complain to and which law applies to their matter.[32] The ALRC is interested in hearing whether the existence of multiple privacy regulators in particular industry sectors and across jurisdictions raises any issues. For example, does the existence of multiple privacy regulators at the federal, state and territory level cause any difficulties in enforcing privacy laws?

---

26 B Bainbridge, *Consultation PC 12*, Canberra, 30 March 2006. See discussion in Ch 8.

27 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 254–255.

28 See discussion in Ch 10 and 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.

29 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.

30 Law Council of Australia Privacy Working Group, *Consultation PC 32*, Sydney, 12 July 2006.

31 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.

32 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 68.

Sharing information

7.18 Inconsistency and fragmentation in privacy regulation can contribute to confusion about how to achieve compliance with privacy regulation and therefore a hesitance by private sector organisations and government agencies to share information. A failure to share information because of privacy concerns can have grave consequences.[33] This issue has been considered by a number of inquiries.[34]

7.19 The Community Services Ministers' Advisory Council (CSMAC) has raised this issue in the context of service provision to vulnerable people. CSMAC has noted that the range of different 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 immediate difficulties with regards to the different standards and requirements that apply, but also in relation to the development of memorandums of understanding and other protocols governing the exchange of information.

7.20 CSMAC gave the following example:

> A protocol has been developed for the exchange of information between state government agencies involved in providing services to homeless people in the inner city of Adelaide. This protocol is based on state privacy requirements and has been signed off, and is being monitored, by the Privacy Committee of South Australia. Non-government organisations, who are major providers of services to homeless people in the inner city, should ideally be included in such a protocol. However, they are outside the jurisdiction of the Privacy Committee. The processes for negotiating inter jurisdictional arrangements covering so many agencies are unclear, and likely to be highly complex and difficult for the service providers involved.[35]

7.21 Real or perceived restrictions in relation to information sharing by government agencies can also impact on business. The Taskforce on Reducing Regulatory Burdens on Business noted that barriers to sharing data between different government agencies can mean that businesses are often required to supply the same information to multiple government agencies which can contribute to compliance burden and cost.[36]

---

33 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

34 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.

35 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

36 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.

Question 7–1 Does the multi-layered regulation of personal information create any difficulties? For example, does the multi-layered regulation of personal information:

(a) cause an unjustified compliance burden;

(b) create problems for organisations that operate in more than one Australian state or territory;

(c) complicate the implementation of programs and services at a national level;

(d) raise any issues in relation to the existence of multiple privacy regulators in particular industry sectors and across the states and territories; or

(e) act as a barrier to the sharing of information between public sector agencies and private sector organisations?

Government contractors

7.22 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 these provisions are inconsistent with the *Privacy Act*. The ALRC is interested in hearing whether privacy provisions in government contracts are contributing to inconsistency and fragmentation in privacy regulation.[37]

Commonwealth contracts

7.23 The *Privacy Act* imposes obligations on agencies entering into contracts to provide services to or on behalf of the agency. Section 95B of the *Privacy Act* 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 practice that would breach the IPPs.

7.24 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.[38] A state or territory authority contracting with an agency will not be covered by the Act. However, the Australian Government Solicitor has advised that notwithstanding this exclusion, agencies need to be mindful of the obligation under IPP 4(b) to ensure that everything

37 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.

38 *Privacy Act 1988* (Cth) s 6D(4)(e).

reasonable is done to prevent unauthorised use or disclosure of personal information when contracting with a state or territory authority.[39]

7.25 Generally the IPPs and not the NPPs will apply to contracted service providers. However, NPP 7 to 10 will apply when a contracted service provider is an organisation under s 6, because the IPPs displace only NPPs 1 to 6—NPPs 7 to 10 have no equivalent IPPs.[40] Further, s 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.

7.26 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 which would be inconsistent with an NPP or an approved code to which it is bound.[41]

7.27 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 which can be investigated by the Privacy Commissioner.[42] However, the standards the Privacy Commissioner would apply in investigating a complaint are those set out in the contract.[43] The Law Council of Australia has noted that:

> This is a matter which is potentially quite confusing for affected individuals who will not necessarily understand what contractual provisions will apply and for the outsourced service providers themselves who will be subject to overlapping and inconsistent regulation.[44]

7.28 The obligations under s 95B extend to a contracted service provider who is not within Australia.[45] Although the Privacy Commissioner could take action overseas to investigate complaints, enforcement of the provisions of the contract overseas may be

---

39 Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 4.

40 Ibid, 3. See discussion of the IPPs and the NPPs in Ch 4.

41 *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.

42 *Privacy Act 1988* (Cth) s 36.

43 Office of the Federal Privacy Commissioner, *Privacy Obligations for Commonwealth Contracts*, Information Sheet 14 (2001).

44 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, 5.

45 *Privacy Act 1988* (Cth) s 5B.

difficult.[46] The ALRC is interested in hearing whether the *Privacy Act* provisions relating to contracted service providers are appropriate and effective.

National consistency issues

7.29 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 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.[47] This may be an issue particularly for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies.

7.30 Telstra advised the OPC Review that the proliferation of state legislation and inconsistency between state and federal legislation have the potential to add costs to conducting business with government agencies.[48] 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.[49]

7.31 Non-government agencies often administer programs that are funded by both the Australian Government and a state or territory. Non-government agencies receiving funding from the Australian Government as well as state or territory governments could find they are caught by state privacy regimes as a result of a protocol or a memorandum of understanding, but also subject to the *Privacy Act* if they are not small business operators. 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.[50]

State and territory contractors

7.32 As noted below, 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 under the various state and territory regimes often resemble the IPPs and NPPs, they are not identical.

---

46 Australian Government Solicitor, *Outsourcing: Agency Obligations Under the Privacy Act*, Legal Briefing No 63 (2002), 4.

47 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.

48 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 37.

49 Ibid, 8 and Rec 5. See Ch 4.

50 Ibid, 38.

7.33 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.[51] Other state regimes provide that compliance with the state privacy regime is subject to any outsourcing arrangements,[52] or are silent on this issue.[53] The ALRC is interested in hearing whether there is a concern that organisations acting under a state or territory contract may not be required to comply with the same privacy standards that are applicable to private sector organisations under the *Privacy Act*.

Question 7–2 Do any issues arise for organisations that provide contracted services involving personal information to Australian Government, state or territory agencies? For example:

(a) are privacy provisions in Australian Government, state or territory agency contracts contributing to inconsistency and fragmentation in privacy regulation;

(b) are the *Privacy Act* provisions relating to Commonwealth contractors appropriate and effective;

(c) do issues arise for Commonwealth contractors that are subject to the NPPs and the IPPs;

(d) do any issues arise for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies;

(e) is there a concern that organisations acting under a state or territory contract may not be required to adhere to the same privacy standards that are applicable to private sector organisations under the *Privacy Act*? If so, how should that concern be addressed?

Interaction of federal, state and territory regimes

7.34 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

51 See, eg, *Information Privacy Act 2000* (Vic) s 17; *Information Act 2002* (NT) s 149.
52 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].
53 See, eg, *Privacy and Personal Information Protection Act 1998* (NSW); South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992).

enact privacy laws.[54] 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.[55] Chapter 2 provides an overview of state and territory privacy laws.

7.35 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.[56] Queensland and South Australia have adopted administrative regimes for the management of personal information in their state public sectors.[57] Western Australia does not have a legislative scheme to regulate personal information, however state freedom of information legislation and public records legislation provides some privacy protection.[58]

7.36 Further, legislation in New South Wales, Victoria and the ACT regulates health information in the public and private sectors.[59] These Acts substantially overlap 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 codes and guidelines.[60] Inconsistency and fragmentation in health privacy regulation is discussed in Chapter 8. The focus of this section is privacy regulation in state and territory public sectors.

Federal, state and territory regimes that regulate personal information

Scope of federal, state and territory regimes

7.37 The *Privacy Act* exempts state and territory authorities from the operation of the *Privacy Act*[61] unless the states and territories request that such authorities be brought into the regime by regulation.[62] State instrumentalities are subject to the private sector

54 The *Privacy Act 1988* (Cth) was passed on the basis of the Australian Government's power to make laws in relation to 'external affairs': *Privacy Act 1988* (Cth) Preamble; *Australian Constitution* s 51(xxix).

55 *Privacy Act 1988* (Cth) s 3 and the *Australian Constitution* are discussed in Ch 2.

56 *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).

57 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).

58 *Freedom of Information Act 1992* (WA); *State Records Act 2000* (WA).

59 *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001* (Vic); *Health Records (Privacy and Access) Act 1997* (ACT).

60 For further discussion see Ch 2 and Ch 8.

61 *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.

62 Ibid s 6F.

provisions of the Act, unless they have been prescribed to fall outside the definition of 'organisation'.[63]

7.38 There is inconsistency, however, in the bodies and individuals regulated under the *Privacy Act* and the state and territory schemes. For example, while a number of state and territory privacy regimes regulate the handling of personal information by state-owned corporations,[64] 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.[65] There is also some 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.[66]

7.39 Further, while legislation in some jurisdictions applies to Ministers,[67] 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.[68] The handling of personal information by local governments is regulated under privacy regimes in some states and territories.[69] However, local governments are not regulated in Queensland[70] or South Australia.[71] Further, universities are subject to personal information laws in some jurisdictions,[72] but not others.[73]

Personal information regulated

7.40 Each of the state and territory regimes contain definitions of 'personal information' that are similar to the definition of the term under the federal Act. While the definitions are similar, they are not identical. For example, whereas the *Privacy Act*

---

63 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].

64 See, eg, *Information Privacy Act 2000* (Vic) s 3; Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1].

65 *Privacy Act 1988* (Cth) s 6C(1).

66 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.

67 See, eg, *Personal Information Protection Act 2004* (Tas) s 3.

68 *Privacy and Personal Information Protection Act 1998* (NSW) s 28(3).

69 For example, Ibid s 3; *Information Privacy Act 2000* (Vic) s 9(1)(d).

70 Queensland Government, *Information Standard 42—Information Privacy* (2001), [1.1] and *Financial Management Standard 1997* (Qld) s 5(2)(c).

71 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.

72 See, eg, *Personal Information Protection Act 2004* (Tas) s 3.

73 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.

and some state and territory regimes require the information to be in material form,[74] the *Privacy and Personal Information Protection Act 1998* (NSW) does not.[75] In other jurisdictions it is unclear whether the personal information has to be recorded in material form to be subject to privacy protection principles.[76]

7.41 Employee records are excluded from the operation of the *Privacy Act*.[77] Some state and territory privacy regimes provide limited protection of employee records.[78] The Personal Information Protection Principles under the *Personal Information Protection Act 2004* (Tas) provide the greatest degree of protection of employee records, subject to a number of exceptions.[79]

7.42 The *Privacy Act* provides limited protection of information held in public registers. IPP 1 places some restrictions on the collection of personal information in a generally available publication.[80] Similarly, the *Information Act 2002* (NT) provides limited protection of information held in public registers.[81] Other jurisdictions, however, provide greater protection for such information. For example, public registers are subject to the Information Privacy Principles under the *Information Privacy Act 2000* (Vic),[82] and the New South Wales legislation prohibits certain disclosures of personal information held in a public register.[83]

Inconsistent principles

7.43 Although the IPPs and the 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.[84] As is noted in Chapter 4, there are significant differences between the IPPs and the NPPs.

7.44 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

---

74 *Privacy Act 1988* (Cth) s 16B; *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.

75 *Privacy and Personal Information Protection Act 1998* (NSW) s 4.

76 The South Australian Government Department of Premier and Cabinet, *PC012—Information Privacy Principles Instruction* (1992) refers to personal information concerning the 'record subject', however, it is unclear whether it requires documents to be in a recorded form.

77 *Privacy Act 1988* (Cth) s 7B(3).

78 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).

79 *Personal Information Protection Act 2004* (Tas) s 10.

80 Similar protection is offered under the Queensland Government, *Information Standard 42—Information Privacy* (2001), [3.1.1].

81 *Information Act 2002* (NT) s 68.

82 *Information Privacy Act 2000* (Vic) s 16(4).

83 *Privacy and Personal Information Protection Act 1998* (NSW) pt 6.

84 See discussion in Ch 2.

Principles under the *Information Privacy Act 2000* (Vic) include principles relating to anonymity and transborder data flows.[85] The Information Standard that applies to the Queensland public sector does not provide for either of these principles,[86] however, the Information Standard that applies to the Queensland Department of Health does.[87]

Regulators

7.45 The nature and functions of privacy regulators vary across the jurisdictions. For example, the *Privacy Act* and other federal legislation provide that the Privacy Commissioner has a number of powers and functions, including powers to investigate and conciliate complaints, and approve and monitor privacy codes and guidelines.[88] 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 the federal Privacy Commissioner.[89] However, the Privacy Committee of South Australia's powers and functions are limited compared to the federal, New South Wales and Victorian privacy commissioners.[90] Some jurisdictions, such as Tasmania and the Northern Territory, have regulators with functions other than oversight of the regulation of personal information.[91]

Remedies

7.46 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,[92] the Victorian Civil and Administrative Tribunal can order compensation of up to $100,000[93] and the Northern Territory Information Commissioner can order compensation up to $60,000.[94] There is no specific provision for compensation under the *Personal Information Protection Act 2004* (Tas). However, the Tasmanian Ombudsman can make any order that he or she considers appropriate on finding a contravention of a

---

85 *Information Privacy Act 2000* (Vic) sch 1.
86 Queensland Government, *Information Standard 42—Information Privacy* (2001).
87 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001), [3.1.8], [3.1.9].
88 See Ch 6 for a discussion of the powers and functions of the Privacy Commissioner.
89 See discussion in Ch 2.
90 However, if a person is dissatisfied with the Privacy Committee's response they are referred to the South Australian Ombudsman: see discussion in Ch 2.
91 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.
92 *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2)(a).
93 *Information Privacy Act 2000* (Vic) s 43.
94 *Information Act 2002* (NT) s 115.

Personal Information Protection Principle.[95] There is no provision for compensation under the Queensland privacy scheme.

Emerging areas of inconsistency and fragmentation

7.47 Inconsistency and fragmentation in privacy regulation continues to emerge as states and territories legislate in areas not covered by the *Privacy Act* or by other state and territory legislation. For example, the *Privacy Act* does not specifically address workplace privacy. New South Wales has recently introduced the *Workplace Surveillance Act 2005* (NSW) to replace the *Workplace Video Surveillance Act 1998* (NSW). The Act prohibits covert surveillance of employees in the workplace without appropriate notice. In 2005, the Victorian Law Reform Commission (VLRC) completed its inquiry into workplace privacy and concluded that the legislative gaps in the protection of workplace privacy required regulation at the state level.[96] The Victorian Parliament has already introduced legislation to implement some of the VLRC's recommendations.[97] While New South Wales and Victoria have initiated these reforms, other state and territory jurisdictions have yet to introduce workplace privacy laws.

State and territory legislation adopting *Privacy Act* provisions

7.48 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.[98]

7.49 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.[99] The ALRC is interested in hearing whether the adoption of *Privacy Act* provisions under state and territory legislation raises any issues. For example, is there confusion about whether the federal Privacy Commissioner or a state or territory privacy regulator has jurisdiction to enforce these laws?

---

95 *Personal Information Protection Act 2004* (Tas) s 22.

96 Victorian Law Reform Commission, *Workplace Privacy: Final Report* (2005), Recs 1–65.

97 See discussion in Ch 2.

98 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.

99 *Road Transport (Vehicle Registration) Regulation 1998* (NSW) reg 15(7).

Residential tenancy databases

7.50 Residential tenancy databases (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.

7.51 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,[100] that information stored on RTDs is sometimes inaccurate,[101] and that tenants sometimes have difficulties in finding out whether they are listed on RTDs.[102]

7.52 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.[103] However, if an RTD operator that is a small business gains consent for the collection or disclosure of an individual's personal information, the *Privacy Act* will not apply.[104] 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.[105]

7.53 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 different jurisdictions.[106] Residential tenancy legislation in New South Wales, Queensland, and now the ACT regulates how real estate agents and lessors list tenants on RTDs.[107] However, this legislation is incomplete and inconsistent. For example, while the *Property Stock and Business Agents Regulation 2003* (NSW) provides for the

---

100 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 87.

101 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), [3.4.8].

102 Victorian Law Reform Commission, *Residential Tenancy Databases* (2006).

103 See *Privacy Act 1988* (Cth) s 6D(4)(c)–(d); Office of the Privacy Commissioner, *Complaint Determination No 3 of 2004*, April 2004.

104 *Privacy Act 1988* (Cth) s 6D(7), (8).

105 Ibid s 18F.

106 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005), [3.2].

107 *Property Stock and Business Agents Regulation 2003* (NSW); *Residential Tenancies Act 1994* (Qld); *Residential Tenancies Act 1997* (ACT).

length of time information can be listed[108] and whether a listed person can access the listing information,[109] the *Residential Tenancies Act 1994* (Qld) does not. In South Australia and the Northern Territory some regulation is provided through fair trading legislation.[110] However, this is primarily consumer protection legislation and does not specifically relate to RTDs.

7.54 A number of inquiries have now recognised the need for national consistency in the regulation of RTDs.[111] In August 2003, the Ministerial Council on Consumer Affairs (MCCA) agreed with 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. However, it was of the view 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.[112]

7.55 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 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. 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 will have primary responsibility for drafting the legislation.

7.56 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 interactions 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 from the RTD operator other privacy obligations, such as those in relation to maintaining accurate records. 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*.

---

108 *Property Stock and Business Agents Regulation 2003* (NSW) sch 6A, cl 6(c).

109 Ibid sch 6A, cl 64(a).

110 See, eg, *Fair Trading Act 1987* (SA) pt 4; *Consumer Affairs and Fair Trading Act 2004* (NT) pt 8.

111 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 Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

112 Ministerial Council on Consumer Affairs/Standing Committee of Attorneys-General Residential Tenancy Database Working Party, *Report on Residential Tenancy Databases* (2005).

7.57 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 *Privacy 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*.[113]

Question 7–3 How should personal information held on residential tenancy databases be regulated? For example, should it be regulated under the *Privacy Act*, by a binding code, or in some other way?

The *Privacy Act* and other federal legislation

7.58 This section examines the interaction of the *Privacy Act* with other federal legislation that regulates personal information. Technical issues such as the use of inconsistent terms are discussed. Other issues discussed include the interaction of the *Privacy Act* with federal legislation that requires or authorises the use or disclosure of personal information, and with secrecy provisions in federal legislation. The interaction of the *Privacy Act* with particular legislative schemes is also considered, for example, the *Freedom of Information Act 1982* (Cth).

Terms and definitions

7.59 Federal legislation in addition to 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 to describe similar information. For example, s 33 of the *Archives Act 1983* (Cth) 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)'.[114] In *Australia's Federal Record: A Review of Archives Act 1983* (ALRC 85), the ALRC concluded that s 33 of the *Archives Act* should be amended to refer to 'personal information'.[115] This recommendation has not been implemented.[116]

---

113 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 6.

114 The *Freedom of Information Act 1982* (Cth) contains a similar exception, however, it refers to 'personal information' so that it remains consistent with the *Privacy Act 1988* (Cth): *Freedom of Information Act 1982* (Cth) s 12(2). See discussion of *Archives Act 1983* (Cth) below. For another example see *Telecommunications Act 1997* (Cth) s 276.

115 Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998), [20.50]–[20.59] and Rec 162. See also Parliament of Australia—House of Representatives

7.60 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. This issue has been raised with the ALRC and in other inquiries and is discussed in more detail in Chapter 10. The ALRC is interested in hearing whether the use of different terms or definitions creates any difficulties.

Question 7–4 Does the inconsistent use of terms and definitions under federal legislation that regulates the handling of personal information create any difficulties? If so, what are some examples of the difficulties created?

Required or authorised by or under law

7.61 An act or practice required or authorised by or under law is an exception to a number of the IPPs and the NPPs.[117] 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.

7.62 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.[118] 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.

7.63 However, the interaction between these provisions and the *Privacy Act* is 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*.[119] Other provisions, such as s 488B of the *Migration Act 1958* (Cth), provide that certain disclosures of information may occur 'even if the

---

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 33.

116 See Question 7–6(e).

117 *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).

118 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.

119 See, eg, *Snowy Hydro Corporatisation Act 1997* (Cth) s 56; *Wheat Marketing Act 1989* (Cth) s 59.

information is personal information (as defined in the *Privacy Act 1988* (Cth)'.[120] Other examples of provisions that require or authorise certain acts or practices are discussed below in relation to specific pieces of federal legislation.

7.64 The ALRC is interested to hear whether the interaction between the *Privacy Act* and provisions under other federal legislation that require or authorise acts or practices that would otherwise be regulated by the IPPs or the NPPs create any difficulties. One issue for consideration is whether the relationship between these provisions and the *Privacy Act* needs to be clarified.

7.65 The House of Representatives Standing Committee on Legal and Constitutional Affairs considered this issue in *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information held by the Commonwealth*.[121] The Committee was concerned that the exceptions to the limitations on the use and disclosure of personal information under IPP 10 and IPP 11[122] may be interpreted as providing additional grounds for use or disclosure. The Committee recommended that the *Privacy Act* be amended to provide that, where an Act other than the *Privacy Act* deals expressly with a matter of permissible use and disclosure, IPP 10 and IPP 11 do not operate to provide additional grounds of disclosure.[123] It was the Committee's view that to allow these additional grounds of disclosure would distort the protective purpose of the *Privacy Act*. It was also of the view that the relationships between these provisions and the *Privacy Act* should be addressed in the *Privacy Act*.[124]

7.66 One issue for consideration is whether provisions in federal legislation that require or authorise certain acts or practices should automatically except certain acts or practices from the operation of the *Privacy Act*.[125] A further issue is whether provisions under federal legislation that require or authorise certain acts or practices involving personal information should be standardised. For example, rules could govern the drafting of such provisions so that certain matters are clearly described, including 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. Another option for consideration is whether the *Privacy Act* should contain a list of provisions

---

120 See also *Customs Act 1901* (Cth) ss 64ACA, 64ACB, 64AF and 273GAB.

121 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).

122 Such as those under *Privacy Act 1988* (Cth) s 14, IPPs 10.1(b), (d); 11.1(c), (e).

123 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), [4.6] and Rec 19.

124 Ibid, [4.6].

125 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 in Ch 3 and in more detail in Ch 5.

in other legislation that requires or authorises certain acts or practices that would otherwise be regulated by the IPPs or the NPPs.

Question 7–5 Do 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? If so, how should the interaction between the *Privacy Act* and these provisions be clarified?

Freedom of Information Act 1982 (Cth)

7.67 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 primarily focused on data protection and provides for transparency only to the extent that it enhances the information privacy rights of individuals.[126]

7.68 The *Privacy Act* and the FOI Act are designed to interact with each other. For example, both Acts use the same definition of 'personal information', and the public sector exemptions under the *Privacy Act* largely mirror the exemptions under the FOI Act.[127] The ALRC is interested in hearing whether the FOI Act and the *Privacy Act* operate effectively together and strike an appropriate balance between the public interest in transparency and the protection of personal information.

Disclosure of personal information

7.69 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.[128] 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).[129] 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

126 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [1.47].

127 See discussion in Ch 5.

128 *Freedom of Information Act 1982* (Cth) s 11.

129 The definition of 'personal information' in the FOI Act corresponds with that in the *Privacy Act 1988* (Cth).

contains his or her own information.[130] However, it does not prevent reliance on the exemption where the information cannot be separated from personal information about another person.[131]

7.70 The exemption under s 41 has been the subject of criticism and commentary.[132] 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 re-worded 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.[133] Other recommendations included that a Freedom of Information Commissioner should issue guidelines to assist agencies to determine whether information is exempt under s 41;[134] and that s 41 should provide that in weighing the public interest in disclosure an agency may have regard to any special relationship between the applicant and the third party.[135] These recommendations have not been implemented.[136]

7.71 An agency may decide to release personal information pursuant to a freedom of information request (FOI request) in some circumstances. IPP 11 imposes 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 applies. A release of personal information pursuant to an FOI request is unlikely to breach IPP 11 as it would be considered to be 'authorised' under law.[137] 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

---

130 *Freedom of Information Act 1982* (Cth) s 41(2).

131 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].

132 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).

133 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.

134 Ibid, [10.8] and Rec 60. See the discussion of a Freedom of Information Commissioner below.

135 Ibid, Rec 61.

136 However, see 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).

137 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 above relating to provisions in federal legislation that require or authorise disclosure.

that is 'required or authorised by law' for the purpose of IPP 11(1)(d).[138] This recommendation has not been implemented.

Access and amendment of records

7.72 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*.[139]

7.73 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'.[140] This did not happen when the *Privacy Act* was enacted in 1988.

7.74 The *Privacy Act* includes provisions to ensure that the access and amendment provisions under both Acts interact with each other.[141] The OPC has expressed the view that the FOI procedures to access and amend information should be used before those under the *Privacy Act*.[142]

7.75 Under IPP 7 an applicant may apply for amendment of personal information on the grounds that it is inaccurate or, given its purpose, is irrelevant, misleading, incomplete or not up-to-date. The FOI Act does not include a reference to 'purpose'.[143] 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 the grounds that the information is irrelevant; where a person seeks deletion of

---

138 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]–[10.24] and Rec 65.

139 *Privacy Act 1988* (Cth) s 35.

140 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].

141 See, eg, *Privacy Act 1988* (Cth) s 34.

142 *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. Other access processes include those under the *Archives Act 1983* (Cth). See discussion below.

143 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [4.17].

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.[144]

7.76 One option for consideration is whether the duplication between the two Acts should be removed. This could be achieved either by repealing the relevant provisions of the FOI Act or transferring the amendment provisions in Part V of the FOI Act to the *Privacy Act*. The ALRC and the ARC considered these options in ALRC 77 and concluded that this overlap did not give rise to any major difficulties.[145] The ALRC and the ARC did recommend, however, several adjustments to the FOI Act to 'ensure the administration of access to and amendment of personal information in the public sector remains satisfactory'.[146] These adjustments included that the amendment procedure in the FOI Act should be amended to remove the requirement of prior legal access and to include the ground of relevance.[147] These recommendations have not been implemented.

7.77 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.[148] However, under the FOI Act 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.[149]

7.78 In ALRC 77, the ALRC and the ARC noted that the potential exists for the Privacy Commissioner to find that, in refusing a person's request to access and amend a document under the FOI Act, the agency breached IPP 6 or IPP 7. The Privacy Commissioner could reach this conclusion independently of any determination by the AAT as to the correctness or otherwise of the agency's decision. The ALRC and the ARC considered that this situation had the potential to create confusion and uncertainty for agencies and to encourage 'forum shopping' by applicants. Accordingly, the ALRC and the ARC recommended that the *Privacy Act* be amended to provide that the Privacy Commissioner is unable to find that an agency has breached IPP 6 or IPP 7 in respect of a decision made under the FOI Act unless that decision has been found on

144 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].

145 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].

146 Ibid, [5.20].

147 Ibid, Recs 77 and 79.

148 *Privacy Act 1988* (Cth) s 35.

149 *Freedom of Information Act 1982* (Cth) s 55.

external review by the AAT or the Federal Court to be incorrect.[150] This recommendation has not been implemented.

Consultation process

7.79 Section 101 of the *Privacy Act* provides that s 27A of the FOI Act applies to access requests made under the *Privacy Act*. Section 27A 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. To assist agencies to determine when a person might reasonably wish to contend that the document is exempt, s 27A(1A) lists factors to which the agency must have regard, including the extent to which the personal information is well known and whether the person to whom the personal information relates is known to be associated with the matters dealt with in the document. One issue is whether the *Privacy Act* should provide for a process of consultation prior to granting access to information that includes personal information about a third party rather than relying on the FOI Act provision. If the *Privacy Act* should provide for a consultation process, a further issue is what that consultation process should be.

A single regulator

7.80 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,[151] and a number of overseas jurisdictions, for example, the Office of the Information and Privacy Commissioner for British Columbia and the United Kingdom Information Commissioner's Office.[152] It has been suggested to the ALRC that a single body should not administer both Acts. Arguably, it would corrupt the focus of each piece of legislation because they aim to achieve different purposes.[153]

7.81 A number of reviews have recommended that a separate body administer the FOI Act. For example, in ALRC 77, the ALRC and the ARC recommended the establishment of a statutory office of Freedom of Information Commissioner.[154] More recently, a report by the Commonwealth Ombudsman has recommended that the Government consider establishing a Freedom of Information Commissioner, possibly

---

150 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [5.22]–[5.23] and Rec 17.

151 See Ch 2.

152 See Office of the Information and Privacy Commissioner for British Columbia, *Website* <www.oipcbc.org> at 28 August 2006; United Kingdom Government Information Commissioner's Office, *Website* <www.ico.gov.uk> at 28 August 2006.

153 N Waters, *Consultation PC 17*, Sydney, 2 May 2006.

154 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.

as a specialised and separately funded unit in the Office of the Commonwealth Ombudsman.[155]

Archives Act 1983 (Cth)

7.82 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).[156] The *Archives Act* provides some protection of information relating to the personal affairs of any person (including a deceased person).[157]

7.83 Further, 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 they are in the open access period or where they 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.[158] The *Archives Act* controls access to these records.

7.84 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 public sector agencies.[159] The *Archives Act* provides for the retention of records. It prohibits the destruction of Commonwealth records without the permission of National Archives, subject to some exceptions.[160]

7.85 One issue for consideration is whether the *Privacy Act* should apply to certain classes of records in the open access period. The ALRC considered this issue in *Australia's Federal Records: A Review of Archives Act 1983* (ALRC 85) and concluded that the application of the IPPs to records more than 30 years old would be needlessly restrictive. The ALRC noted that the exemption categories within the archives legislation would continue to provide appropriate protection for personal information.[161]

---

155 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].

156 *Archives Act 1983* (Cth) s 31.

157 Ibid s 33. See discussion above.

158 See the definition of 'record' in *Privacy Act 1988* (Cth) s 6.

159 See discussion in Ch 4.

160 See generally *Archives Act 1983* (Cth) ss 24–29.

161 Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983*, ALRC 85 (1998), [15.56].

A single information Act?

7.86 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.[162] 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.[163]

7.87 Another option for consideration is whether the FOI Act, the *Privacy Act* and the *Archives Act* should be consolidated into a single Act. An example of such an Act is the *Information Act 2002* (NT). The ALRC and the ARC in ALRC 77 considered the amalgamation of these Acts. 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 proposal met with strong opposition in submissions to the review and was ultimately rejected. The ALRC and ARC did recommend, however, that the Acts should be amended, where necessary, to ensure that together they provide a cohesive and consistent package of legislation on government records.[164]

Tax file number legislation and data-matching

7.88 The handling of tax file numbers (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.[165] 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).[166]

7.89 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.[167]

---

162 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).

163 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].

164 Ibid, [5.6].

165 Subject to exceptions: *Taxation Administration Act 1953* (Cth) pt III div 2 subdiv BA.

166 The regulation of tax file numbers is discussed in Ch 12. Secrecy provisions governing the use of TFNs are discussed below.

167 Office of the Privacy Commissioner, *Data-Matching* <www.privacy.gov.au/act/datamatching> at 21 June 2006.

7.90 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.[168] Section 12 of the Act requires the Privacy Commissioner to issue guidelines for the conduct of the data-matching program. The *Data-matching Program (Assistance and Tax) Guidelines* came into effect in April 1997.[169] 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.[170] In the event of a complaint being made it is dealt with in accordance with the provisions of Part V of the *Privacy Act*.[171] One issue is whether federal legislation relating to the handling of TFNs and data-matching should be consolidated under the one Act, in particular the *Privacy Act*.

7.91 The Privacy Commissioner has also issued the advisory guidelines *The Use of Data-matching in Commonwealth Administration* for adoption by agencies conducting data-matching that is not regulated by the *Data-matching Act*. The guidelines are not legally binding. The ALRC is interested in hearing whether data-matching programs that fall outside the *Data-matching Act* should be regulated by legislation, rather than the guidelines.[172]

Census and Statistics Act 1905 (Cth)

7.92 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).[173] 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. The ALRC is interested in hearing whether personal information collected for the purposes of the *Census and Statistics Act* is adequately protected.

7.93 In the late 1970s, the ALRC conducted an inquiry into privacy issues and the census, culminating in the release in 1979 of *Privacy and the Census* (ALRC 12).[174] The report made a number of recommendations directed to the protection of personal

168 *Data-matching Program (Assistance and Tax) Act 1990* (Cth) pt 2.
169 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).
170 *Privacy Act 1988* (Cth) s 14.
171 Ibid s 14.
172 As recommended in 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), [4.10] and Rec 23.
173 *Census and Statistics Act 1905* (Cth) s 8.
174 Australian Law Reform Commission, *Privacy and the Census*, ALRC 12 (1979).

information collected as part of the census.[175] A number of these recommendations have been implemented.[176]

7.94 Following the release of ALRC 12 the *Privacy Act* was enacted. The *Privacy Act* applies the IPPs to personal information collected as part of the census.[177] For example, personal information collected by the ABS for a census is likely to be regarded as collection for a lawful purpose directly related to a function or activity of the ABS and necessary and directly related to that purpose.[178] 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.[179] For example, s 19A provides that the 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.[180]

7.95 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.[181] 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 to be preserved for release for future research after a closed access period of 99 years.[182]

7.96 Another recent development is the Census Data Enhancement (CDE) project.[183] 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[184] and a Privacy Impact Assessment (PIA) was prepared.[185] Although

---

175 Ibid, x–xvi.

176 See, eg, *Census Information Legislation Amendment Act 2000* (Cth).

177 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 House of Representatives Legal and Constitutional Affairs Committee—Parliament of Australia, *Saving Our Census and Preserving Our History* (1998), Ch 4.

178 *Privacy Act 1988* (Cth) s 14, IPP 1.1.

179 *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.

180 See House of Representatives Legal and Constitutional Affairs Committee—Parliament of Australia, *Saving Our Census and Preserving Our History* (1998), Rec 1. See also Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

181 *Census Information Legislation Amendment Act 2000* (Cth).

182 Explanatory Memorandum, Census Information Legislation Amendment Bill 2006 (Cth).

183 Australian Bureau of Statistics, *Census of Population and Housing—Census Data Enhancement* <www.abs.gov.au> at 25 August 2006.

184 Australian Bureau of Statistics, *Enhancing the Population Census: Developing a Longitudinal View* (2005).

there was some support for the project, a number of submissions and the PIA identified significant privacy-related concerns.[186] 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 possible 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.[187]

7.97 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.[188] The SLCD will now be based on a 5% sample of the population. It is the ABS's view that the reduction of the dataset to a 5% sample will make the dataset unsuitable for administrative and other non-statistical uses. Despite the modifications, the APF still have a number of concerns about the proposal, including that data collected in each census will now be retained and linked, will cover one million people, and may be used in conjunction with data from other sources.[189]

Corporations Act 2001 (Cth)

7.98 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. Under the Act, companies, registered schemes and persons who maintain registers on behalf of companies and registered schemes must allow anyone to inspect these registers.[190] 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.

7.99 A submission to the Inquiry stated that the provisions relating to access to registers under the *Corporations Act* are contrary to the NPPs.[191] It was submitted that

---

185 Pacific Privacy Consulting, *Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics* (2005).

186 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].

187 Pacific Privacy Consulting, *Census Enhancement Project: Privacy Impact Assessment Report for Australian Bureau of Statistics* (2005), 3.

188 Australian Bureau of Statistics, 'ABS Develops a New View of Records Across Successive Censuses' (Press Release, 18 August 2005).

189 Australian Privacy Foundation, *Privacy Concerns with the 2006 Census* (2006) <www.privacy.org.au/Campaigns/Census> at 24 August 2006.

190 *Corporations Act 2001* (Cth) s 173.

191 Link Market Service, *Submission PR 2,* 24 February 2006.

under the *Privacy Act*, a company that maintains a member's register cannot provide personal information except for the primary purpose of managing a member's 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 Security holder Reference Number) but can allow access to a register to a member of public if they visit our offices to a view a register (in this process they can see a specific individual's holding balance).[192]

7.100 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,[193] and that access to this information will encourage misuse of this information.[194]

7.101 Section 168 of the *Corporations Act* is an example of a provision that requires or authorises the disclosure of information for the purposes of the *Privacy Act*. Therefore, it is unlikely that compliance with the *Corporations Act* requirements would breach NPP 2. However, the ALRC is interested in whether it is appropriate that disclosure of a shareholder's personal details, including his or her share holdings, is a disclosure of personal information that is permitted for the purposes of NPP 2.

Commonwealth Electoral Act 1918 (Cth)

7.102 Part VI of the *Commonwealth Electoral Act 1918* (Cth) 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*.[195] The Act also requires the provision of electoral roll information to a number of different individuals and organisations, including members of Parliament and political parties.[196]

7.103 The *Commonwealth Electoral Act* and the *Privacy Act* provide the legislative privacy framework governing the electoral roll. 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

---

192 Ibid.

193 See Information Integrity Solutions, *Customer Lists: Background Paper for CUSCAL Industry Association* (2005).

194 Credit Union Industry Association and others, *Issues Overview: Member Registers, Takeovers and Mutuals* (2006).

195 *Commonwealth Electoral Act 1918* (Cth) ss 90, 90A.

196 Ibid s 90B.

information contained in a roll. Disclosure to political organisations for these permitted purposes would constitute a secondary purpose of disclosure that is authorised by law for the purposes of the *Privacy Act*.[197]

7.104 One issue for consideration is whether the provisions under the *Commonwealth Electoral Act* and the *Privacy Act* provide adequate protection of personal information, particularly in relation to 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 protections such as security and retention. These issues are dealt with in the NPPs. However, the NPPs do not apply to acts or practices carried out by political organisations and their contractors, subcontractors and volunteers in relation to electoral matters.[198] Issues related to this exemption are discussed in detail in Chapter 5. Privacy concerns related to developments in technology and the use of public registers such as the electoral roll are discussed in Chapter 11.

Anti-Money Laundering and Counter-Terrorism Financing Bill 2006

7.105 On 13 July 2006, the Minister for Justice and Customs, Senator the Hon Chris Ellison, released for public consultation a revised exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) (AML/CTF Bill 2006) and draft Anti-Money Laundering and Counter-Terrorism Financing Rules (AML/CTF Rules).

7.106 The AML/CTF Bill 2006 is intended to enable individual businesses to manage money laundering and terrorism financing risks. The Bill 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'.[199] A large number of 'designated services' are listed in the Bill including opening an account, making a loan, and supplying goods by way of hire purchase.[200]

7.107 The Bill requires a reporting entity to carry out a procedure to verify a customer's identity before providing a designated service to the customer.[201] In addition, reporting entities must give the Australian Transaction Reports and Analysis Centre (AUSTRAC) reports about suspicious matters,[202] and must have and comply

197 *Privacy Act 1988* (Cth) s 14, IPP 10.1(c).
198 Ibid s 7C.
199 Revised Exposure Draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) cl 5.
200 Ibid cl 6.
201 Ibid pt 2.
202 Ibid pt 3.

with an anti-money laundering and counter-terrorism financing program.[203] The Bill also imposes various record-keeping requirements on reporting entities.[204] For example, a reporting entity must make a record each time it provides a designated service and must retain the record for seven years.[205]

7.108 Part 11 of the Bill relates to secrecy and access. Except as permitted by the Bill, an AUSTRAC official, a customs officer or a police officer must not disclose information or documents obtained under the Bill.[206] 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 cl 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.[207] The Bill requires designated agencies, including state and territory agencies, to comply with the IPPs in respect of the accessed AUSTRAC information.[208]

7.109 The revised exposure draft AML/CTF Bill 2006 and draft AML/CTF Rules reflect consideration of over 120 submissions provided to the Attorney-General's Department following the release of the first exposure Bill on 16 December 2005,[209] and the findings of the Senate Legal and Constitutional Legislation Committee inquiry into the exposure draft Bill.[210] 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.[211] These recommendations have not been included in the latest revised exposure draft of the Bill.

7.110 Submissions in response to the revised exposure draft AML/CTF Bill 2006 continue to raise privacy issues. For example, the OPC and the APF have both observed that while Part 11 of the Bill imposes some privacy obligations on state and territory agencies accessing AUSTRAC information, not all states and territories have

---

203 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 face when providing designated services in Australia that might involve or facilitate money laundering or financing of terrorism: Ibid cl 74.

204 Ibid pt 10.

205 Ibid cl 85.

206 See, eg, Ibid cl 93.

207 Ibid cl 99.

208 Ibid cl 99(3).

209 See Australian Government Attorney-General's Department, *Welcome to Anti-money Laundering Reform Online* <www.ag.gov.au> at 27 August 2006.

210 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Financing Bill 2005* (2006).

211 Ibid, [4.72]–[4.76].

enacted privacy regimes. Therefore, it is unclear whether individuals will be able to make complaints and seek remedies if information has been dealt with inappropriately by these agencies.[212]

7.111 Submissions have also noted that the NPPs may not provide adequate protection of personal information collected and disclosed under the Bill. For example, reporting entities that are 'organisations' for the purposes of the *Privacy Act* will have to comply with the NPPs. However, the NPPs will generally not apply to reporting entities that are small businesses.[213] A proportion of the reporting entities that are collecting and sharing personal information for the purposes of the Bill therefore may not be subject to any privacy regulation.

7.112 Under Part 10 of the Bill a reporting entity must retain for seven years information contained in a suspicious matter report to AUSTRAC. However, the Bill prevents an individual from seeking access to that information under NPP 6. The OPC has therefore suggested that, as an individual is not able to check information that is held about his or her, and has no opportunity to provide clarifying details or correct errors, further limitations on the retention of information by reporting entities are warranted.[214] It has also been observed that cl 110 of the Bill makes it an offence to provide a designated service on an anonymous basis. This directly contradicts NPP 8 which provides that wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.[215]

7.113 The Attorney-General's Department is currently reviewing the submissions received during the second consultation period and is finalising the legislative package for introduction to Parliament later in 2006. The ALRC is interested in views on how the Bill interacts with the *Privacy Act* and whether the Bill adequately protects personal information.

---

212 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*, 3; Australian Privacy Foundation, *Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006*, August 2006, 57.

213 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*, 3–4; Australian Privacy Foundation, *Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006*, August 2006, 62; Chartered Secretaries Australia, *Submission to the Attorney-General's Department Consultation on the Second Exposure Draft of the Anti-Money Laundering and Counter-Terrorism Funding Bill 2006*, August 2006.

214 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*, 4.

215 Ibid, 5.

Question 7–6 Does the interaction between the *Privacy Act* and other federal legislation that regulates the handling of personal information require clarification? In particular:

(a) does 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;

(b) should the *Privacy Act* provide for a process of consultation prior to granting access to information that includes personal information about a third party rather than rely on the process outlined in the *Freedom of Information Act 1982* (Cth);

(c) should the *Privacy Act* and the *Freedom of Information Act 1982* (Cth) be administered by the same body;

(d) should the *Privacy Act* apply to certain classes of records in the open access period for the purposes of the *Archives Act 1983* (Cth);

(e) should the exemption under the *Archives Act 1983* (Cth) relating to 'information relating to the personal affairs of any person' be amended to provide an exemption in relation to 'personal information' as defined in the *Privacy Act*;

(f) should the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth) be consolidated in one Act;

(g) should federal legislation relating to the handling of tax file numbers and data-matching be consolidated in one Act? If so, should they be consolidated in the *Privacy Act*;

(h) should data-matching programs that fall outside the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) be more formally regulated;

(i) is personal information collected pursuant to the *Census and Statistics Act 1905* (Cth) adequately protected;

(j) is it 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;

(k) does the *Commonwealth Electoral Act 1918* (Cth) provide adequate protection of personal information included on the electoral roll;

(l) does the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) adequately protect personal information?

Secrecy and confidentiality

7.114 This section considers the relationship between secrecy provisions and the provisions under Part VIII of the *Privacy Act*.

Secrecy

7.115 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.

7.116 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. However, those interests may sometimes be conflicting. For example, a person may want to access his or her personal information to check that it has been correctly recorded and is not being disclosed without his or her consent; but to grant that access could intrude upon the secrecy interests of the institution.

7.117 There are a number of provisions in federal legislation that create general offences in relation to the unauthorised disclosure of official information.[216] There are also a large number of secrecy provisions in federal legislation that deal with unauthorised disclosure of information in specific circumstances.[217] Secrecy provisions in federal legislation are criminal offences that attract criminal penalties designed to deter. The *Privacy Act*, however, operates as an administrative regime that allows for private remedies such as the award of compensation.

---

216 See, eg, *Crimes Act 1914* (Cth) ss 70 and 79; *Criminal Code Act 1995* (Cth) s 91.1.

217 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.

7.118 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 'protected information' acquired in the course of his or her duties as an 'officer' to any person or to a court. '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.

7.119 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 law to refuse to provide an individual with access to a record.[218] 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.[219] 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.[220]

7.120 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.[221] However, other provisions do not address this issue.[222]

7.121 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 *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 thought that the transfer of personal information between Commonwealth agencies should be regulated by the *Privacy Act*,

---

218 *Privacy Act 1988* (Cth) s 14, IPP 6.

219 Ibid s 14, IPP 11.1(d).

220 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.

221 *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)'.

222 See, eg, *Disability Services Act 1986* (Cth) s 28.

rather than by the secrecy provisions in specific statutes.[223] 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*.[224]

7.122 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.[225] In August 2006, the Treasury released a discussion paper *Review of Taxation Secrecy and Disclosure Provisions*.[226] The Discussion Paper proposes the standardisation and consolidation of the disparate rules under tax legislation that impose strict obligations on tax officers and others who receive tax information.[227] One issue being considered by the review is the relationship between the secrecy and disclosure provisions under tax legislation and the *Privacy Act*.[228]

Question 7–7 Do 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, should the *Privacy Act,* rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by Australian Government agencies?

Part VIII of the Privacy Act (obligations of confidence)

7.123 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.[229] It generally preserves all other laws,

---

223 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] and Rec 17.

224 Ibid, [4.6] and Rec 19. See discussion above under 'Required or authorised by or under law'.

225 See Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Ch 5 and Recs 5–1 to 5–5.

226 Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006).

227 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.

228 Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions: Discussion Paper* (2006), Appendix D.

229 *Privacy Act 1988* (Cth) s 90.

principles or rules 'under or by virtue of which an obligation of confidence exists', 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'.[230] Part VIII therefore allows for the fact that obligations of confidence may arise in various ways. Section 89 also provides broadly that the Part only applies to an obligation 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'.[231]

7.124 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.

7.125 Section 93 concerns relief for breach of the obligation. Without limiting any other right a confider has to relief in respect of a breach,[232] 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'.[233] 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'.[234]

Question 7–8 Are the provisions in Part VIII of the *Privacy Act* necessary? If so, are the provisions adequate and should they be contained in the *Privacy Act* or elsewhere?

Privacy rules, codes and guidelines

7.126 Various privacy rules, codes and guidelines regulate the handling of personal information in addition to the *Privacy Act* and state and territory legislation.[235] The ALRC is interested in hearing whether these instruments contribute to fragmentation and inconsistency in the regulation of personal information.

---

230 Ibid s 91.
231 Ibid s 89.
232 Ibid s 93(2).
233 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.
234 *Privacy Act 1988* (Cth) s 93(3).
235 See Ch 2.

7.127 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.[236]

7.128 A number of these 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.[237] There is no overlap with the NPPs as a code replaces the NPPs for those organisations bound by the code. 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 code and is therefore subject to the *Privacy Act* or a state or territory privacy regime in relation to these activities.

7.129 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,[238] and another in relation to politically motivated violence.[239] The former contains guidelines on the treatment of personal information.[240]

7.130 While the guidelines are generally consistent with the *Privacy Act*, there are differences. For example, Guideline 4.1 provides that requests by ASIO for access to personal information held by Commonwealth agencies should be 'limited to that which is reasonably necessary for the purposes of approved investigations'. This guideline is more permissive than IPP 1(1)(b) which requires that collection of information must be

---

236 *Privacy Act 1988* (Cth) s 16A.

237 Biometrics Institute, *Biometrics Institute Privacy Code—Public Register* (2006) <www.biometricsinstitute.org> at 4 September 2006, 16–18.

238 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/attorney.htm> at 10 August 2006.

239 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/attorney.htm> at 22 July 2006, Guideline 3.2.

240 Ibid.

'necessary'. Further, unlike the IPPs, the guidelines do not provide for access or alteration of records containing personal information.

7.131 The acts or practices of ASIO relating to personal information are completely exempt from the operation of the *Privacy Act*, therefore ASIO is not subject to two inconsistent privacy standards.[241] However, the guidelines are an example of privacy regulation that imposes different standards to the *Privacy Act*. The ALRC is interested in hearing whether the rules and guidelines that regulate privacy in relation to intelligence agencies are adequate and appropriate.[242]

7.132 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.[243] The Code includes a schedule that outlines principles to govern fair conduct relevant to consumer data protection.[244] 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 usage 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.

7.133 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. However, *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.[245]

7.134 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 customer information about the supply of each service separately. The Law Council

---

241 *Privacy Act 1988* (Cth) s 7(1)(a)(i)(B), (2)(a).

242 Privacy rules can also be issued by the responsible Ministers under *Intelligence Services Act 2001* (Cth) s 15 for the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation and the Defence Signals Directorate. See discussion in Ch 5.

243 Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2001), [6]. For further discussion of the Code see Ch 1.

244 Ibid, sch E.

245 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.

argues that this is a much higher standard than the reasonable expectation test under NPP 2.1(a), and that this illustrates how the incorporation of NPP-like requirements into state legal regimes can lead to divergence over time.

Question 7–9 Do privacy rules, privacy codes and privacy 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?

8. Health Services and Research

Contents

Introduction

8.1 In a submission to the Office of the Privacy Commissioner (OPC) review of the private sector provisions of the *Privacy Act 1988* (Cth) (OPC Review) 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]

8.2 Traditionally, patients' personal health information was 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 may also be subject to secrecy provisions in legislation discussed below.

8.3 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]

8.4 In addition, 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 are frequently 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 rather than personal details on test request forms.[7]

8.5 More recently, privacy legislation has been introduced in a number of Australian jurisdictions specifically to regulate the handling of personal health information.[8]

---

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).

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).

Health service providers continue to be subject to secrecy provisions and duties of confidentiality and, 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]

8.6 While this Issues Paper is concerned primarily with the privacy regime, other ethical and legal duties imposed on health service providers will be considered in the context of the need for greater national consistency. State and territory health privacy legislation and the draft *National Health Privacy Code*[10] will also be considered in this context. An overview of privacy regulation in the states and territories, including health privacy regulation, is provided in Chapter 2.

Health information privacy

A separate regime for health information?

8.7 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 Information Privacy Principles (IPPs) in handling personal information. The IPPs do not draw a distinction between personal information and health information.[11]

8.8 The *Privacy Amendment (Private Sector) Act 2000* (Cth) and the National Privacy Principles (NPPs) set out in that Act, however, do draw a distinction between personal information and 'sensitive information'. Sensitive information is defined to include 'health information about an individual' and is given a higher level of protection under the NPPs than personal information generally. 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.[12] 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;

---

9 M McMahon, 'Re-thinking Confidentiality' in I Freckelton and K Petersen (eds), *Disputes & Dilemmas in Health Law* (2006) 563, 583.

10 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003).

11 The IPPs and NPPs are discussed in detail in Ch 4.

12 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].

- the rights contained in the Bill enabling individuals to access their own health information were inadequate; and

- the Bill created inconsistent standards governing privacy rights in the public and private sectors.[13]

8.9 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.[14]

8.10 The House of Representatives Standing Committee concluded that health information should be included in the Bill.[15] However, the Committee expressed concern about 'the resulting plethora of principles that will then apply to both the public and private health sectors'[16] and went on to recommend 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.[17]

8.11 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 different and separate set of principles.

8.12 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 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 Working Group and provided specialist advice.[18]

8.13 The framework developed by the Working Group has become known as the *National Health Privacy Code*. The draft Code contains 11 National Health Privacy

---

13 Ibid, [6.12].
14 Ibid, [6.7]–[6.10].
15 Ibid, Rec 15.
16 Ibid, [6.35].
17 Ibid, Rec 14.
18 Phillips Fox, *Report on Public Submissions in Relation to Draft National Health Privacy Code* (2003), 1.

Principles (NHPPs) and additional detailed procedures for providing individuals with access to their health information.[19]

8.14 Although the NHPPs have much in common with the NPPs, there are also many 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,[20] NHPP 4 requires health service providers to retain health information for at least seven years.[21]

8.15 In consultation, the Victorian Health Services Commissioner 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. Because of the nature of the information, the relationship between a health consumer and a health service provider is based on trust and must be protected to ensure that those in need of health services access those services without being put off by concern about their privacy.[22]

8.16 The Victorian *Health Records Act 2001* provides a separate set of Health Privacy Principles (HPPs) that expressly deal with some of the issues that arise in the health services and health and medical research contexts. Like the NHPPs the HPPs require the retention of health information records for at least seven years.[23] 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;[24] the use of health information in research;[25] the transfer of health information to another health service provider when the consumer changes health service provider; and arrangements for the custody of health information when a health service provider closes.[26] These issues are discussed further below but are included here to indicate the sort of issues that may be addressed in a separate set of principles.

8.17 Before proceeding to examine the question of national consistency in the handling of health information, the ALRC would be interested in hearing whether

---

19 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003). The Code is discussed in more detail, below.

20 *Privacy Act 1988* (Cth) sch 3, NPP 4.2.

21 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 4.2.

22 Victorian Government Office of the Health Services Commissioner, *Consultation PC 28*, Melbourne, 9 May 2006.

23 *Health Records Act 2001* (Vic) sch 1, HPP 4.

24 Ibid sch 1, HPP 2.2(f).

25 Ibid sch 1, HPP 2.2(g).

26 Ibid sch 1, HPP 10.

health information is so unique that it requires a different set of privacy principles, (such as the NHPPs), separate from the principles used to regulate other sensitive personal information.

Question 8–1 Does the regulation of health information require a different and separate set of privacy principles to those used to regulate other sensitive personal information?

National consistency: issues and problems

8.18 Chapter 2 provides an overview of privacy regulation in Australia. The view 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. A number of the states and territories have also passed legislation that regulates the handling of health information in the state or territory public sector and/or the private sector.[27] The following table provides a general view of the jurisdictional scope of health privacy legislation in Australia.

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 8.19 below]	*Privacy Act 1988* (Cth)
Western Australia		*Privacy Act 1988* (Cth)

27 *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).

South Australia	[See 8.20 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)

8.19 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*[28] is based on the IPPs and *Information Standard 42A on Information Privacy for the Queensland Department of Health*[29] is based on the NPPs. Both standards are issued under the *Financial Management Standard 1997* (Qld).

8.20 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. There does not seem to be similar formal administrative policies in place in Western Australia.

8.21 As indicated in the table above, a number of jurisdictions have both a federal Act and a state or territory Act regulating the handling of health information. 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 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 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.[30]

---

28 Queensland Government, *Information Standard 42—Information Privacy* (2001).

29 Queensland Government, *Information Standard 42A—Information Privacy for the Queensland Department of Health* (2001).

30 Explanatory Memorandum, Health Records (Privacy and Access) Bill 1997 (ACT).

8.22 The scope of the state and territory legislation may also be different to the scope of the federal legislation. For example, the Victorian *Health Records Act*—unlike the *Privacy Act*—covers small business operators and employee records.

8.23 The requirement to comply with similar but different legislation adds to the costs and complexity of compliance for private sector health service providers and health and medical researchers. In addition, health consumers in those jurisdictions are faced with two sets of principles and two possible avenues of complaint.

8.24 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.

8.25 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. 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.

8.26 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 when 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.[31] These issues, including the need for a single set of principles in the *Privacy Act*, are discussed in detail in Chapter 4.

8.27 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;

---

31 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.

- confusion about which regime regulates particular businesses;
- forum shopping to exploit differences in regulation; and
- uncertainty among consumers about their rights.[32]

8.28 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 understanding and meeting respective obligations, as well as confusion for health consumers affected by dual legislative instruments.[33]

8.29 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.[34]

8.30 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.[35] Some submissions expressed concern that the problem will become worse as electronic health records become commonplace.[36]

8.31 In the 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 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

---

32 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.

33 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.

34 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.

35 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

36 Ibid, 43.

> genetic information. This would be achieved most effectively by developing nationally consistent rules for handling all health information.[37]

National consistency: some proposed solutions

8.32 As discussed in Chapter 2, 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.
>
> 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.[38]

8.33 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'.[39]

8.34 As discussed in Chapter 2, however, s 3 of the *Privacy Act* clearly 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 were 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.

8.35 An amendment of the kind suggested by the OPC would be aimed at ensuring that state and territory legislation purporting to regulate the handling of personal information in the private sector—including the relevant provisions of the *Health Records and Information Privacy Act*, the *Health Records Act* and the *Health Records (Privacy and Access) Act*—would be invalid. The intent would be to ensure as far as possible that private sector health service providers and health and medical researchers would only be required to comply with one regime.

8.36 Any attempt by the Australian Parliament to 'cover the field' in this way would raise complex political and constitutional issues. For example, it would be necessary to consider the implications for the plethora of other state and territory legislation dealing

---

37 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.

38 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 45.

39 Ibid, Rec 2.2.

with health information privacy, such as notification requirements in public health legislation.

8.37 In addition, while it may address the problems caused by the fact that more than one set of privacy principles apply to the handling of health information in the private sector, it would not address the problems caused by the fact that different privacy principles apply in the public sector. The following section will consider whether it is possible to ensure that health information is regulated in a consistent way across the public and private sectors in every Australian jurisdiction.

Question 8–2 Should s 3 of the *Privacy Act* be amended to state that the Act is intended to regulate the handling of health information in the private sector to the exclusion of state and territory legislation?

National Health Privacy Code

8.38 Part 1 of the draft *National Health Privacy Code* provides that:

> The main objects of this Code are:
>
> (a) to achieve national consistency in the handling of health information across the private and public sectors through the establishment of a single national code for the appropriate collection and handling of health information by public and private sector organisations; and
>
> (b) to do so in a way that:
>
> (i) ensures responsible and appropriate collection and handling of health information held in the public and private sectors;
>
> (ii) achieves a balance between the public interest in protecting the privacy of health information with the public interest in the legitimate use of that information;
>
> (iii) enhances the ability of individuals to be informed about their health, disability or aged care services;
>
> (iv) promotes the provision of quality health, disability and aged care services; and
>
> (v) engenders consumer and provider trust in the protection of health information privacy.[40]

8.39 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 and in every Australian state and

40 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 1 cl 2.

territory, including in relation to research or the compilation or analysis of statistics.[41] The content of the draft Code included detailed provisions in relation to access to health information and 11 NHPPs similar to the HPPs in the Victorian *Health Records Act*.[42]

8.40 Following a public consultation process, a revised version of the Code—as well as draft mandatory guidelines for research, and draft explanatory notes for the use or disclosure of genetic information—was developed,[43] but was not made publicly available. Consequently, where provisions of the draft Code are discussed in this Issues Paper, references are to the provisions of the draft Code released for public comment in 2003. DOHA advised the OPC Review that the content of the draft Code had been finalised and would be considered by Health Ministers in 2005.[44]

8.41 On that basis, the OPC made the following recommendations:

> The Office urges the National Health Ministers' Council to finalise the National Health Privacy Code. This should include agreement by all jurisdictions on the contents of the code and on its consistent implementation in each jurisdiction.[45]
>
> The Australian Government should consider adopting the National Health Privacy Code as a schedule to the Privacy Act. This would recognise the Australian Government's part in the consistent enabling of the Code. Should agreement not be reached by all jurisdictions about implementing the Code, the Australian Government should still consider adopting the code as a schedule to the Act to provide greater consistency of regulation for the handling of health information by Australian Government agencies and the private sector.[46]

8.42 While much of the content of the draft Code apparently has been finalised, it has not yet been formally endorsed at ministerial level[47] and, as at July 2006, an implementation mechanism had not been agreed.[48]

8.43 Chapter 2 of this Issues Paper considers in detail the various mechanisms by which a nationally consistent regime for the handling of personal information might be achieved; for example, through national legislation or some form of cooperative scheme involving the Australian Parliament and the states and territories. Cooperative schemes include:

---

41 Ibid, pt 1 cl 1, pt 2 div 2.

42 Ibid. The text of the draft *National Health Privacy Code* (2003) can be found at <http://pandora.nla.gov.au/tep/44612>.

43 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

44 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.

45 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 12.

46 Ibid, Rec 13.

47 Australian Government Department of Health and Ageing, *Correspondence*, 17 August 2006.

48 National E-Health Transition Authority, *NEHTA's Approach to Privacy*, Version 1.0 (2006).

- a referral of power by the states to the Australian Parliament under s 51(xxxvii) of the *Australian Constitution*;

- mirror legislation, where one jurisdiction passes legislation and the other jurisdictions enact similar legislation; and

- applied legislation, where one jurisdiction passes legislation, which is then applied by the other jurisdictions as a law of those jurisdictions.[49]

National health privacy legislation

8.44 As discussed in Chapter 2, the Australian Parliament probably has the power to pass national legislation regulating the handling of personal information throughout Australia based on a range of constitutional powers, including the external affairs power. Such legislation could regulate the handling of personal information in both the public and private sectors—including information handled by the state and territory public sectors—subject to certain express and implied constitutional limits.

8.45 The relevant international instruments—such as the *International Covenant on Civil and Political Rights*[50] (ICCPR) and the Organisation for Economic Cooperation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[51] (OECD Guidelines)—that provided the basis for the exercise of the external affairs power by the Australian Parliament in passing the *Privacy Act*, do not expressly provide for the protection of health information. In order to provide a firm constitutional basis for national health privacy legislation, it would be necessary to establish that the legislation was an appropriate means of giving effect to the international obligations in these and other relevant international instruments.[52] Difficulties might arise, for example, if the national health privacy legislation included principles that were not consistent with the principles set out in the international instruments.

8.46 Alternatively, it would be necessary to demonstrate that the protection of health information was 'a matter of international concern'.[53] There is evidence of international concern in relation to the protection of health information, both as a

---

49 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005).

50 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

51 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980).

52 *Commonwealth v Tasmania* (1983) 158 CLR 1; *Richardson v Forestry Commission* (1988) 164 CLR 261.

53 *Commonwealth v Tasmania* (1983) 158 CLR 1.

subset of personal information and in specific contexts—such as electronic health initiatives, HIV/AIDS, and genetic information.[54]

8.47 It may also be possible to rely to some extent on s 51(xxiiiA) of the *Australian Constitution* to provide a basis for federal health privacy legislation. Section 51(xxiiiA), so far as it is relevant, provides that the Australian Parliament may make laws in relation to 'the provision of … pharmaceutical, sickness and hospital benefits, medical and dental services (but not so as to authorize any form of civil conscription)'. It is important to note, however, that s 51(xxiiiA) does not give the Australian Parliament unlimited power to regulate the relationship between health service providers and health consumers generally. Any such exercise of legislative power must relate to medical or dental services provided by the Australian Government or to pharmaceutical, sickness or hospital benefits.[55]

8.48 To proceed with national legislation without the agreement of the states and territories is likely to give rise to political and constitutional issues, particularly if the legislation is expressed to extend to the state and territory public sectors. If, however, it were agreed by all jurisdictions that national legislation was an appropriate and effective way forward in this area, the states and territories could be given the opportunity to opt in to the scheme. State and territory public sector authorities currently fall outside the definition of 'agency' in the *Privacy Act* and are specifically excluded from the definition of 'organisation'. States and territories may request, however, that their public sector authorities be brought into the regime by regulation.[56]

8.49 Alternatively, states might refer the protection of personal health information to the Commonwealth under s 51(xxxvii) of the *Australian Constitution*.[57]

Co-operative schemes

8.50 An alternative to national health privacy legislation is some form of co-operative scheme involving applied or mirror legislation. Co-operative schemes currently operate in a number of areas—such as trade practices and competition law—in which there is shared responsibility for the subject matter between the federal and state and territory governments. A number of these are discussed in Chapter 2. The OPC Review noted in relation to the draft *National Health Privacy Code* that national consistency would require every state and territory to adopt the Code unamended.[58] This could be achieved through applied or mirror legislation.

---

54 See, eg, United Nations and International Telecommunications Union World Summit on the Information Society, *Plan of Action*, WSIS-03/GENEVA/DOC/5-E (2003); United Nations Economic and Social Council, *Genetic Privacy and Non-Discrimination*, Resolution 2004/9 (2004); European Commission EuroSOCAP Project, *European Standards on Confidentiality and Privacy in Healthcare* (2005).

55 *General Practitioners Society v Commonwealth* (1980) 145 CLR 532.

56 *Privacy Act 1988* (Cth) s 6F. Note, however, that to date, only four state public sector authorities have been brought into the scheme in this way: see Ch 5.

57 Referral of matters to the Commonwealth by the states is discussed in Ch 2.

58 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 69.

8.51 A model of applied legislation in which a national Code has been established as the foundation for a nationally consistent regime is found in the *Agricultural and Veterinary Chemicals Code Act 1994* (Cth). In that Act, the Code was expressed to apply only in the ACT. Each of the states and the Northern Territory then enacted legislation applying the Code as a law of the relevant state or the Northern Territory.[59]

8.52 A model of mirror legislation followed a report by the ALRC, *Human Tissue Transplants* (ALRC 7).[60] The *Transplantation and Anatomy Act 1978* (ACT) was passed, implementing the major recommendations of the report. It enacted a new definition of death, framed in terms of the irreversible loss of brain function, and provided legislative regulation of the removal of human tissue for transplantation, post-mortem examinations and for use in schools of anatomy. Mirror legislation was then passed in every other state and territory. This regime did not involve federal law.[61]

8.53 The OPC also expressed the view that there would need to be a process to ensure ongoing co-operation in relation to the draft *National Health Privacy Code* and that the National Health Privacy Working Group and AHMAC could play this role.[62] The need to ensure ongoing consistency is important where consistency is achieved through mirror or applied legislation. This is because it is possible for each jurisdiction to amend its own legislation without reference to other jurisdictions. The report *Uniform Evidence Law* (ALRC 102) recommended in relation to the uniform Evidence Acts that:

> To promote and maintain uniformity, the Standing Committee of Attorneys-General (SCAG) should adopt an Intergovernmental Agreement which provides that, subject to limited exceptions, any proposed changes to the uniform Evidence Acts must be approved by SCAG. 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.[63]

8.54 A similar agreement could be developed in relation to core elements of any national health privacy scheme, using AHMAC and Australian Health Ministers rather than the Standing Committee of Attorneys-General (SCAG) to develop and implement the Intergovernmental Agreement.

---

59 M Farnan, 'Commonwealth-State Cooperative Schemes: Issues for Drafters' (Paper presented at 4th Australasian Drafting Conference, Sydney, 3–5 August 2005).

60 Australian Law Reform Commission, *Human Tissue Transplants*, ALRC 7 (1977).

61 *Human Tissue Act 1983* (NSW); *Human Tissue Act 1982* (Vic); *Transplantation and Anatomy Act 1979* (Qld); *Human Tissue and Transplant Act 1982* (WA); *Transplantation and Anatomy Act 1983* (SA); *Human Tissue Act 1985* (Tas) and the *Human Tissue Transplant Act 1979* (NT).

62 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 43.

63 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Rec 2–1.

A schedule to the Privacy Act

8.55 As noted above, the OPC recommended a fall back option in relation to the draft *National Health Privacy Code*. If agreement could not be reached by all jurisdictions about implementing the draft Code, the Australian Government should consider adopting the Code as a schedule to the *Privacy Act* to provide greater consistency of regulation for the handling of health information by Australian Government agencies and the private sector.[64]

Question 8–3 Is the draft *National Health Privacy Code* an effective way to achieve a nationally consistent and appropriate regime for the regulation of health information? If so, what is the most effective model for implementing the draft *National Health Privacy Code*? If not, what other model should be adopted to achieve a nationally consistent and appropriate regime for the regulation of health information?

Question 8–4 If the draft *National Health Privacy Code* is not implemented nationally, should the Australian Government adopt the Code as a schedule to the *Privacy Act*?

Electronic health information systems

8.56 Traditionally, health information has been collected and stored in paper-based systems, with information about one individual held in a number of disparate locations, for example, in general practitioners' records, hospital records, pathology laboratory records and medical specialists' records. Health information is increasingly collected, stored and transferred in electronic form, for example: many health service providers, including hospitals, now hold health information in electronic health information systems; health service providers, such as pathologists, communicate test results and other health information electronically; and health information about large numbers of health consumers is collected into central databases, such as the Medicare database and cancer registers, discussed further below.

8.57 Chapter 12 discusses the privacy issues and problems that arise in electronic environments, in particular, around the use of unique identifiers, access, data linkage, data quality, transfer and security. The same issues arise in relation to health information in electronic health information systems. In addition, and as discussed above, such information is regularly transferred between the public and private sectors and across jurisdictional boundaries and is subject to complex and overlapping privacy regulation.

---

64 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 13.

8.58 Another issue that has arisen in the health information context, is recent initiatives 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.

Health*Connect* and NEHTA

8.59 In its submission to the OPC Review, DOHA stated that:

> 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.[65]

8.60 Health*Connect* is a national 'change management strategy'—involving the Australian, state and territory governments—aimed at developing standardised electronic health information products and services and common standards so that health information can be exchanged securely between health service providers. The Australian Government has provided funding to help certain health service providers—general practitioners, Aboriginal Community Controlled Health Services, and community pharmacies—to obtain high-speed broadband internet connections. This is intended to facilitate their participation in Health*Connect* and similar initiatives.[66]

8.61 The National E-Health Transition Authority (NEHTA) has responsibility for the development of a national interoperability framework. NEHTA is jointly funded 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 that future electronic health systems purchased by Australian governments are compliant with NEHTA's interoperability requirements.[67]

---

65 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.

66 Australian Government Department of Health and Ageing, *Broadband for Health* <www.health.gov.au/ehealth/broadband> at 30 August 2006.

67 National E-Health Transition Authority, *About NEHTA* <www.nehta.gov.au> at 30 August 2006.

8.62 NEHTA is also developing the national foundations for Shared Electronic Health Records—records that will contain selected health information about a health consumer, which can be shared among multiple authorised health service providers.

8.63 NEHTA initiatives include:

- establishing standard clinical terms for use by e-health systems, so that systems use consistent terminology to describe the same disease, therapy, medicine and so on;

- identifying a secure means of electronically transferring health information between authorised health service providers;

- designing specifications for secure electronic health records, to enable authorised health service providers to view the collated health history of a health consumer while maintaining high standards of privacy; and

- developing unique identifiers for health consumers—the Individual Healthcare Identifier (IHI)—health service providers—the Health Provider Identifier (HPI)—and medical products, so that the right information is assigned to the right health consumer.[68]

8.64 NEHTA has undertaken to release a *Privacy Blueprint* for the HPI and IHI as well as one for the Shared Electronic Health Record during 2006. These are intended to be detailed action plans applied to each specific initiative.[69] As noted in Chapter 12, the Council of Europe has stated that policy makers should evaluate carefully the costs and benefits of any scheme involving the use of unique identifiers.[70] In the case of existing schemes using unique identifiers, it has recommended that restrictions be placed on the use of the identifiers to ensure that the scheme achieves 'the requisite balance between privacy and administrative efficiency'.[71]

8.65 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*, the first pilot of an electronic health records system, to be run in the Hunter region.[72] Health*Connect* South Australia is developing an electronic planning and referral system for health consumers with

---

68 National E-Health Transition Authority, *Fact Sheet: A National Interoperability Framework for E-Health* (2006) <www.nehta.gov.au> at 1 September 2006. See also Ch 12 on unique multi-purpose identifiers.

69 National E-Health Transition Authority, *NEHTA's Approach to Privacy*, Version 1.0 (2006), 7.

70 Council of Europe, *The Introduction and Use of Personal Identification Numbers: The Data Protection Issues* (1991).

71 Ibid. The issues involved in the use of unique identifiers are discussed in detail in Ch 12.

72 J Hatzistergos (New South Wales Minister for Health), 'Trial of Electronic Health Records' (Press Release, 23 March 2006).

chronic disease.[73] Health*Connect* Northern Territory has commenced implementation of a Shared Electronic Health Record Service.[74]

8.66 The Health*Connect* website states that:

> The implementation of the Health*Connect* strategy in your state or territory will respect the privacy of personal health information. Privacy, confidentiality and security are paramount and the Australian Government will ensure that wherever the Health*Connect* strategy is implemented, the electronic transfer of your health information will comply with existing legislative and regulatory requirements, the professional ethical and legal obligations of health care providers as well as the latest technical advances in security measures.
>
> Existing legislation will need to be reviewed to comply with the changes to e-health technology to ensure protection of individual's records.[75]

8.67 In a submission to the OPC Review, DOHA noted that

> as personal information becomes more widely dispersed and stored on larger databases, it may potentially become more difficult for an individual to control the flow and exchange of personal information unless proper privacy safeguards are built in from the outset.[76]

8.68 The OPC 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.[77]

8.69 NEHTA has stated that:

> Technology is, on the whole, privacy neutral. It is the business drivers behind a technology and the incentive to exploit security flaws in its implementation that will determine the key privacy risks. By building privacy into the design of e-health systems, including proactively identifying and addressing potential security flaws, NEHTA believes that national e-health infrastructure can and will meet privacy requirements.[78]

---

73 Australian Government Department of Health and Ageing, *HealthConnect: FAQs* <www.healthconnect.gov.au> at 30 August 2006.

74 Ibid.

75 Ibid.

76 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.

77 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.

78 National E-Health Transition Authority, *NEHTA's Approach to Privacy*, Version 1.0 (2006), 5.

8.70 The ALRC would be interested in hearing from stakeholders in relation to these issues and, in particular, whether electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or those proposed in the draft *National Health Privacy Code.*

Question 8–5 Do electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or the draft *National Health Privacy Code*?

Medicare and Pharmaceutical Benefits

8.71 An example of existing electronic health records held by the Australian Government are the databases 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*.

8.72 Section 135AA of the *National Health Act 1953* (Cth)[79] 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. The section only applies 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.[80]

8.73 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.[81]

79 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.

80 Commonwealth, *Parliamentary Debates*, House of Represenatives, 30 May 1991, 4490 (P Staples—Minister for Aged Family and Health Services).

81 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.

8.74 The Privacy Commissioner first issued the *Medicare and Pharmaceutical Benefits Program Privacy Guidelines* in 1993 and they were last amended in 2000.[82] The Guidelines are legally binding and a breach of the Guidelines is an 'interference with privacy' that may provide the basis for a complaint to the Privacy Commissioner.[83] 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).

8.75 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.[84] 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.[85]

8.76 In November 2004, the Privacy Commissioner announced a major review of the Guidelines.[86] The review was 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.[87] An issues paper[88] 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.

8.77 The major issues canvassed in the course of the review were:

- the separation of claims information collected under the Medicare and Pharmaceutical Benefits programs;

---

82 Ibid. 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.

83 *Privacy Act 1988* (Cth) s 13(bb); *National Health Act 1953* (Cth) s 135AB.

84 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.

85 Ibid, Commissioner's Note on cl 1.4.

86 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).

87 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.

88 Office of the Privacy Commissioner, *Review of the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issues Paper* (2004).

- the circumstances under which claims information from each program may be linked;
- the periods for which claims information may be retained;
- the use of claims information for medical and other research purposes;
- the handling by DOHA of claims information that does not identify individuals; and
- the application of the Guidelines to agencies other than Medicare Australia and DOHA.[89]

8.78 The Privacy Commissioner's final report was issued in August 2006 and includes 25 findings. 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;[90]
- the prohibition against storing Medicare and Pharmaceutical Benefits claims information on the same database should apply to all agencies;[91]
- changes should be made to the periods for which Medicare Australia may retain claims information in linked and unlinked form;[92] and
- some changes are required in the way DOHA may handle claims information.[93]

8.79 In light of this comprehensive and recent review of the Guidelines by the OPC, the ALRC's preliminary view is that it is not necessary to conduct another detailed study of the Guidelines. However the ALRC is interested in views about the review findings. A complete list of the review's findings can be found in the OPC's final report, which is published on the OPC website.[94]

---

89 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.

90 Ibid, Finding 2.

91 Ibid, Finding 23.

92 Ibid, Findings 6–8.

93 Ibid, Findings 14–21.

94 Ibid. See Office of the Privacy Commissioner, *Review of the Medicare and PBS Privacy Guidelines issued under section 135AA of the National Health Act 1953* <www.privacy.gov.au/health/guidelines/healthreview.html>, 26 September 2006.

8.80 Finally, the Privacy Commissioner's review focused on the Guidelines themselves and expressly excluded the enabling provisions in the *National Health Act* including the legislative requirement that information collected in connection with the Medicare and Pharmaceutical Benefits programs is stored in separate databases.[95] For this reason, the ALRC would be interested in views on these provisions and whether the role provided for the Privacy Commissioner by the *National Health Act* is an appropriate and effective one.

Question 8–6 The *National Health Act 1953* (Cth) requires the Privacy Commissioner to issue guidelines in relation to the handling of personal information collected in connection with claims under the Medicare Benefits Program and the Pharmaceutical Benefits Program. Is this an appropriate and effective role for the Privacy Commissioner?

Privacy Act 1988 (Cth)

8.81 In the absence of a nationally consistent health privacy regime, the *Privacy Act* remains central to the protection of this information in the Australian Government and ACT public sectors and in the private sector. As noted above, the IPPs do not distinguish between 'personal information', 'sensitive information' and 'health information'—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. Whether there is a need for a single set of privacy principles applying to both agencies and organisations is discussed in detail in Chapter 4.

8.82 The 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 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.[96] This issue is discussed further below.

8.83 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.[97] 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

95 Ibid, 12.
96 *Privacy Act 1988* (Cth) s 6D(4)(b).
97 Ibid sch 3, NPP 10.

consumer would reasonably expect the information to be used in this way.[98] There is also special provision in the NPPs for:

- the disclosure of health information to an individual's family member or guardian where the individual is physically or legally unable to consent to disclosure;[99]
- the use of health information in medical research relevant to public health or safety;[100]
- the use of health information in the compilation and analysis of statistics relevant to public health and safety;[101] and
- the use of health information in the management, funding or monitoring of a health service.[102]

8.84 These issues are discussed further below.

Health information

8.85 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.

8.86 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
>
> (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.[103]

98 Ibid sch 3, NPP 2.1(a)(i).
99 Ibid sch 3, NPP 2.4–2.6.
100 Ibid sch 3, NPPs 2.1(d), 10.3(a)(i).
101 Ibid sch 3, NPPs 2.1(d), 10.3(a)(ii).
102 Ibid sch 3, NPP 10.3(a)(iii).
103 Ibid s 6.

8.87 In ALRC 96, the ALRC and AHEC 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 these existing definitions. 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.[104] 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.[105]
>
> The Commonwealth should amend s 6 of the *Privacy Act* to define 'sensitive information' to include human genetic test information.[106]

8.88 In its response to ALRC 96, the Australian Government expressed support for these recommendations in principle. The *Privacy Legislation Amendment Act 2006* (Cth) was passed in September 2006. 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.[107]

8.89 The Government also noted in its response to ALRC 96 that the recommendation in relation to 'health information' had been considered in the context of the draft *National Health Privacy Code*,[108] however, the provision dealing with genetic information in the draft Code is not the same as the recent amendments to the *Privacy Act*. The other major difference in the definition in the draft Code is that it expressly includes information about mental or psychological health. The definition of 'health information' in the draft Code is as follows:

> (a) information or an opinion about:
>
> (i) the physical, mental or psychological health (at any time), of an individual; or
>
> (ii) a disability (at any time) of an individual; or

---

104 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [7.75].

105 Ibid, Rec 7–4.

106 Ibid, Rec 7–5.

107 *Privacy Legislation Amendment Act 2006* (Cth) sch 2 s 2.

108 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 2 August 2006, 7.

(iii) an individual's expressed wishes about the future provision of health services to him or her; or

(iv) 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; or

(d) genetic information about an individual in a form which is, or could be, predictive (at any time) of the health of the individual or any other individual (including antecedents or descendants)—but does not include health information, or a class of health information or health information contained in a class of documents, that is prescribed as exempt health information in accordance with the Code.[109]

8.90 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*[110] contain the same 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.[111]

8.91 The ALRC would be interested in hearing whether the definition of 'health information' developed for the draft *National Health Privacy Code* is appropriate and effective and whether it should replace the existing definition in the *Privacy Act*.

Health service

8.92 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

---

109 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4, cl 1.

110 *Health Records and Information Privacy Act 2002* (NSW) s 6; *Health Records Act 2001* (Vic) s 3; *Information Act 2002* (NT) s 4.

111 *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary.

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

(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.[112]

8.93 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.

8.94 The definition in the Victorian *Health Records Act* is very similar to the definition in the draft Code.[113] The definitions in the ACT health records legislation and the Northern Territory *Information Act* have many of the same elements[114] but the New South Wales legislation 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.[115]

8.95 The ALRC would be interested in hearing whether the definition developed for the draft *National Health Privacy Code* is appropriate and effective and whether it should replace the existing definition in the *Privacy Act*.

---

112 *Privacy Act 1988* (Cth) s 6.
113 *Health Records Act 2001* (Vic) s 3.
114 *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary; *Information Act 2002* (NT) s 4.
115 *Health Records and Information Privacy Act 2002* (NSW) s 4.

Question 8–7 Are the definitions of: (a) 'health information'; and (b) 'health service' in the draft *National Health Privacy Code* appropriate and effective? Should the *Privacy Act* be amended to adopt these definitions?

Agencies and organisations

8.96 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. However, there are a number of significant exemptions that mean that some agencies and organisations holding health information may not be subject to the *Privacy Act* in relation to that information. These exemptions are discussed in detail in Chapter 5.

8.97 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. This exemption means that the great majority of Australian businesses—approximately 94%[116]—are exempt from the *Privacy Act*. Small businesses operators that pose a higher risk to privacy, however, have been brought back into the regime. For example, 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; or
- disclose personal information for a benefit, service or advantage; or
- provide a benefit, service or advantage to collect personal information.[117]

8.98 Small businesses that hold health information and provide a health service are bound by the NPPs. This leaves open the possibility, however, that small businesses that hold health information but do not provide health services—for example, health data registers that simply store health information—may not be required to comply with the Act.

8.99 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 *Privacy Act* to justify amending the Act to make it clear that all small businesses that

116 See detailed discussion in Ch 5.

117 *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.

hold genetic information are subject to its provisions. In ALRC 96, the ALRC and AHEC recommended that:

> The Commonwealth should amend the *Privacy Act* to ensure that all small business operators that hold genetic information are subject to the provisions of the Act.[118]

8.100 In its response to ALRC 96, the Australian Government did not support this recommendation. The Government considered 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 unfairly burdened by the costs and processes of complying with privacy legislation.[119]

8.101 The draft *National Health Privacy Code* is expressed to apply to 'every organisation that is a health service provider or collects, holds or uses health information'.[120] The Victorian *Health Records Act* applies to organisations that are health service providers or collect, hold or use health information[121] and does not exempt small business operators. The New South Wales *Health Records and Information Privacy Act* exempts small business operators by reference to the *Privacy Act.*[122]

8.102 The ALRC strongly remains of the view that the *Privacy Act* should be amended to ensure that all small businesses that hold genetic information are covered by the Act, and would be interested in hearing whether this position should be extended to cover health information more generally.

8.103 Chapter 5 discusses those Australian Government agencies that are partly or wholly exempt from the *Privacy Act*. These include the Defence Intelligence Group in the Department of Defence; the various intelligence agencies; federal courts; federal industrial tribunals; the Australian Crime Commission; royal commissions; the Integrity Commissioner; and a range of other miscellaneous organisations listed in Schedule 2 to the *Freedom of Information Act 1982* (Cth). The ALRC would be interested in hearing whether any of these agencies should be required to comply with the *Privacy Act* in relation to health information.

---

118 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.

119 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 2 August 2006, 8.

120 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 2 div 1 cl 1.

121 *Health Records Act 2001* (Vic) s 11.

122 *Health Records and Information Privacy Act 2002* (NSW) s 4.

Question 8–8 Should the *Privacy Act* be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act?

Management, funding and monitoring

8.104 In its submission to the OPC Review, the NHMRC stated that health information was important in three areas: the provision of health services; the conduct of research; and management activities. The NHMRC noted that management activities might include, for example: quality assurance; quality improvement; policy development; planning; evaluation; and cost benefit analysis.[123]

8.105 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 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.

8.106 Health information may only be collected without consent for these activities in limited circumstances. First, 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*.

123 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.

8.107 The NHMRC has noted that it is often difficult to distinguish quality assurance activities in the health care context from research[124] and is of the view that, where management activities amount to research, they should always be conducted in accordance with the Section 95A Guidelines and be subject to review by a Human Research Ethics Committee (HREC).[125] The NHMRC has published some guidance on how to make the distinction between quality assurance and research.[126] It may be that, for the purposes of the *Privacy Act*, particular activities should be classified as both management activities and research and should be subject to review by an HREC. However, where management activities do not amount to research, it seems illogical to require that they be approved by a HREC. The conduct of medical research is discussed in detail below.

8.108 While NPP 10 has tried to accommodate the use of health information without consent for management, funding and monitoring purposes, there appear to be some gaps. These activities are undertaken in both the health services and research contexts, yet NPP 10.3 only expressly refers to management, funding and monitoring of a health service.

8.109 In addition, management activities are undertaken in both the public and the private sectors. The IPPs do not make specific reference to management, funding and monitoring activities and so it is necessary to rely on the basic principles to decide whether it is possible to use health information in the public sector for such activities.

8.110 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. This would seem to allow collection by public sector health service providers or researchers for management, funding and monitoring activities directly related to the agency's activities. The NPPs allow collection of health information without consent in the circumstances described above for the management, funding and monitoring of a health service; that is, the collection would have to be regulated in some way by law, professional guidelines or the Section 95A Guidelines. The NPPs are not clear, however, in relation to the management, funding and monitoring of research projects.

8.111 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*

---

124 Ibid.

125 Ibid. National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

126 National Health and Medical Research Council, *When Does Quality Assurance in Health Care Require Independent Ethical Review?* (2003).

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.[127]

8.112 This also may be the case in relation to research projects, although this is not stated in the Information Sheet. IPP 11 allows disclosure of health information without consent for management activities where the individual concerned is reasonably likely to have been aware that health information was usually disclosed in this way. The OPC Review expressed the view that disclosure of health information for management activities would generally be within people's reasonable expectations.[128]

8.113 NPP 2 allows 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. As noted above, the OPC considers that this would be the case in relation to some management, funding and monitoring activities. However, in response to concerns that the position is not clear, the OPC Review recommended that:

> The Office will issue guidance in relation to NPP 2 to clarify that organisations can disclose health information for the management, funding and monitoring of a health service.[129]

8.114 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.[130] 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 for management activities under these Acts does not, however, depend on establishing that it is a directly related secondary purpose or that it would be within the individual's reasonable expectations.

8.115 While it appears that collection, use and disclosure of health information for the management, funding and monitoring of health services may be allowed under both the IPPs and the NPPs, the position is not sufficiently clear. It is less clear in relation to the management, funding and monitoring of research projects, particularly under the NPPs.

---

127 Office of the Federal Privacy Commissioner, *Handling Health Information for Research and Management*, Information Sheet 9 (2001).

128 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

129 Ibid, Rec 61.

130 *Health Records and Information Privacy Act 2002* (NSW) sch 1, HPP 10; *Health Records Act 2001* (Vic) sch 1, HPP 2.2.

The ALRC would be interested in hearing whether further guidance by the OPC is an appropriate and effective response to concerns in this area—given that any such guidance will not be binding—or whether further action, for example, an amendment of the *Privacy Act* is necessary. In addition, the ALRC would be interested in hearing whether the management, funding and monitoring of research should be treated in the same way as the management, funding and monitoring of health services.

Question 8–9 Is guidance by the Office of the Privacy Commissioner to clarify that organisations can disclose health information for the management, funding and monitoring of a health service an appropriate and effective response to concerns in this area? If not, what is an appropriate and effective response?

The provision of health services

8.116 The following section deals with the impact of the *Privacy Act* on the provision of health services to health consumers. In consultation, it was suggested 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 a team of health professionals treating the individual.[131] This may be a result of actual problems with the *Privacy Act*, which are discussed below in relation to particular privacy principles, or it may be for other reasons. For example, the Act may have a chilling effect on the sharing of information based on a misunderstanding of the Act or the privacy principles.

8.117 In its submission to the OPC Review, 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

131 NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006.

> health information without explicit consent, and implementing ineffective and inefficient procedures in their efforts to comply with the law.[132]

8.118 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.[133] It may be that further action or changes are necessary to ensure an appropriate balance is found between individual privacy and the effective delivery of health services to consumers. The ALRC would be interested in case studies or other evidence from stakeholders that indicate whether and to what extent the regulation of personal health information, and the *Privacy Act* in particular, is impeding the provision of appropriate health services to individuals.

Question 8–10 Is there evidence that the regulation of personal health information impedes the provision of appropriate health services to individuals? If so, what changes are necessary to facilitate the provision of appropriate health services?

Consent

8.119 Consent is a central concept in the *Privacy Act* and is of particular importance in dealing with health information because of the personal and sensitive nature of that information. Consent allows the individual health consumer to retain control of his or her health information. This contributes to an 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 health 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.

8.120 The issue of consent is also being considered in the context of Health*Connect*. NEHTA is responsible for developing a consent framework for Health*Connect*.[134]

8.121 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

---

132 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.

133 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.

134 National E-Health Transition Authority, *About NEHTA* <www.nehta.gov.au> at 30 August 2006.

- the individual must have the capacity to understand and communicate their consent.[135]

Express and implied consent

8.122 'Consent' is defined in the *Privacy Act* as 'express or implied consent'.[136] Express consent 'refers to consent that is clearly and unmistakably stated'.[137] 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.[138]

Consent in the IPPs and the NPPs

8.123 Consent is generally required when collecting health information under the NPPs.[139] Consent is not, however, required when collecting health information under the IPPs.[140] Consent is not required for use under the NPPs or the IPPs if health information is used for the purpose 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.[141] Consent is required, however, if health information is to be used for a purpose that is not directly related to the purpose of collection.[142]

8.124 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.[143] Consent is not required for disclosure under the NPPs if the information is disclosed for the purpose it was collected or a directly related purpose and individuals would reasonably expect the organisation to disclose health information in that way.[144]

8.125 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

---

135 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A5.2.
136 *Privacy Act 1988* (Cth) s 6.
137 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A5.3.
138 Ibid, Guideline A5.3.
139 *Privacy Act 1988* (Cth) sch 3, NPP 10.1.
140 Ibid s 14.
141 Ibid s 14, IPP 10.1; sch 3, NPP 2.1.
142 Ibid s 14, IPP 10.1; sch 3, NPP 2.1.
143 Ibid s 14, IPP 11.1.
144 Ibid sch 3, NPP 2.1.

use is necessary to lessen or prevent a serious and imminent threat to an individual's life or health;[145] or where the use is required or authorised by law[146] or reasonably necessary to enforce the criminal law.[147]

8.126 There is also a regime established to allow health information to be used without consent for research in some circumstances. This regime is discussed in detail below.

8.127 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.

Specific and general consent

8.128 Consent runs from the very specific to the very general, along a wide spectrum. 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 4.

8.129 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 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. But consent should not be so general as to undermine the requirements that it be voluntary and adequately informed.

Capacity

8.130 Significant issues arise when individuals may 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. Children may have limited capacity to understand and consent. Capacity to consent and decision-making disabilities in relation to the handling of personal information generally are discussed in Chapter 9.

8.131 The IPPs do not make specific provision for this situation. Under the IPPs, health information may be collected without consent and used for the purpose it was collected and any other directly related purpose without consent. The NPPs do make specific provision for the collection and disclosure of health information about an

145 Ibid s 14, IPP 10.1(b); sch 3, NPP 2.1(e).
146 Ibid s 14, IPP 10.1(c); sch 3, NPP 2.1(g).
147 Ibid s 14, IPP 10.1(d); sch 3, NPP 2.1(h).

individual when the individual in question is physically or legally incapable of giving consent or cannot communicate consent. In particular, the NPPs allow health service providers to collect health information where this is necessary to prevent or lessen a serious and imminent threat to the life or health of an individual who is incapable of giving consent.[148]

8.132 Health service providers may disclose health information to a parent, child, or other specified family member or guardian if the disclosure is necessary to provide appropriate treatment or care for the health consumer, or for compassionate reasons, and the disclosure is not contrary to the known wishes of the health consumer.[149] The OPC Review stated that these principles are intended to give health service providers a discretion to disclose the health information of an individual with impaired decision-making capacity when, broadly speaking, it is in the individual's interest to do so.[150]

8.133 The OPC also noted that where a guardianship or administration tribunal has made an order appointing someone to act on an individual's behalf, disclosure of relevant health information about the individual to the guardian or administrator would be 'authorised by law'.[151]

8.134 Submissions to the OPC Review noted that the *Privacy Act* sometimes causes problems for carers conducting business on behalf of persons with decision-making disabilities. The OPC noted that, while the NPPs allow for disclosure to carers in some circumstances,

> the Privacy Act does not guide the organisation in whether or not to provide information to carers, family members or other responsible persons. This is a matter for the organisation's professional judgement in line with its own policies and other legal obligations in the circumstances of each case.[152]

8.135 In response to these concerns, the OPC Review recommended that:

> The Office will, in recognition that disclosures of health information under NPP 2 are appropriately permitted in law but may not occur in practice, develop further and more practical guidance.[153]

8.136 Privacy NSW has developed a *Best Practice Guide on Privacy and People with Decision-Making Disabilities*,[154] that provides detailed guidance on these matters. The

148 Ibid sch 3, NPP 10.1(c).
149 Ibid sch 3, NPP 2.4–2.6.
150 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.
151 *Privacy Act 1988* (Cth) sch 3, NPP 2.1(g). Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 214.
152 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.
153 Ibid, Rec 64.
154 Privacy NSW, *Best Practice Guide: Privacy and People with Decision-Making Disabilities* (2004).

Guidelines include discussion about capacity, consent and involving individuals in decision making about their privacy. The Guidelines are not limited to decision making in relation to health information and are discussed further in Chapter 9.

8.137 The draft *National Health Privacy Code* includes detailed provisions allowing an 'authorised representative' to give consent to the collection, use or disclosure of health information on behalf of an individual who is incapable of giving consent. An 'authorised representative' is defined as:

> (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.[155]

8.138 The draft Code also defines 'incapable of giving consent' as follows:

> 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.[156]

8.139 The draft 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.[157] The ALRC would be interested in hearing whether these provisions provide a more appropriate and effective framework than the *Privacy Act* for handling health information where an individual has limited capacity to give consent.

---

155 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), pt 4 cl 1.

156 Ibid, pt 4 cl 4.

157 Ibid, pt 4 cl 4.

Question 8–11 Does the *Privacy Act* provide an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent? Does the draft *National Health Privacy Code* provide a more appropriate and effective framework for handling health information in these circumstances?

Question 8–12 Are there any other issues relating to consent to deal with health information in the health services context that the ALRC should consider?

Collection of health information

Collection of family medical history information by health service providers

8.140 NPP 10.1 provides that, subject to a number of exceptions, an organisation must not collect health information without consent. In December 2001, the Privacy Commissioner received an application from a health service provider for a public interest determination under s 73 of the *Privacy Act*.[158] The provider was concerned 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. The IPPs do not require that agencies have consent before collecting health information and so the same issue did not arise.

8.141 On 21 December 2001, the Privacy Commissioner made two Temporary Public Interest Determinations (TPIDs) in response to these concerns. The TPIDs were given effect for up to 12 months, to permit the Privacy Commissioner to conduct consultations on the issue as required by Part VI of the *Privacy Act.* Over 60 submissions were received during the consultation period, and a conference was held to consider a draft determination in August 2002.[159] 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, because the public interest in its continuation substantially outweighed the public interest in adhering to NPP 10.1:

> 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,

158 Office of the Privacy Commissioner, *Public Interest Determinations* <www.privacy.gov.au/act/publicinterest/index.html> at 27 August 2006. Public interest determinations are discussed further in Ch 6.

159 *Privacy Act 1988* (Cth) s 76 provides for a conference to be held to consider a draft determination on the Privacy Commissioner's initiative.

> and notifying those individuals about these collections, would be impractical, inefficient and detrimental to the provision of quality health outcomes.[160]

8.142 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

- the third party's information is relevant to the family, social or medical history of that consumer.[161]

8.143 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.

8.144 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.[162]

8.145 NHPP 1 of the draft *National Health Privacy Code* specifically provides for the collection of health information without consent where

> 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

---

160 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 274.

161 Privacy Commissioner, *Public Interest Determination 9*, effective 11 December 2002; Privacy Commissioner, *Public Interest Determination 9A*, effective 11 December 2002.

162 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.

(ii) from a relative or carer of the individual;[163] or

(iii) in any other situation, in accordance with any guidelines issued for the purposes of this paragraph.[164]

8.146 The OPC Review recommended that:

> The Australian Government should consider amending NPP 10 to include an exception that mirrors the operation of Public Interest Determinations 9 and 9A.[165]

Question 8–13 Should the *Privacy Act* be amended to allow health service providers to collect information about third parties without their consent in line with Public Interest Determinations 9 and 9A? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of such information than the current provisions of the *Privacy Act*?

Collection of family medical history information by insurance companies

8.147 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.[166]

8.148 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

---

163 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 Ch 9.

164 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 1.1(i).

165 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), Rec 81.

166 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), [28.49].

> genetic relatives for use in underwriting insurance policies in relation to those applicants.[167]

8.149 The OPC Review noted that, to date, the Privacy Commissioner had not considered an application for a PID in these terms[168] 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.[169]

8.150 The ALRC would be interested in views in relation to these issues and 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.

Question 8–14 Should the *Privacy Act* 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?

Collection of health information without consent

8.151 As noted above, NPP 10.1 provides in part that an organisation must not collect health information without consent except in a number of specified situations. One of those is where 'the collection is required by law'.

8.152 NPP 10.2 provides another 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
>
> (ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the organisation.

167 Ibid, Rec 28–3.
168 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 276.
169 Ibid, Rec 82.

8.153 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.[170] 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 AIDS.[171]

8.154 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'.

8.155 NPP 2.1(g) allows disclosure of health information without consent where this is 'required or authorised by or under law'. The OPC Review expressed the concern that

> the more restrictive provisions of NPP 10.2(b)(i), especially in the context of health service delivery, have the potential to unduly impede the effective delivery of such services. The restrictive character of this sub-paragraph may be inconsistent with the *Privacy Act*'s general reliance upon the ethical traditions, including recognition of the duty of confidentiality, of health service providers.
>
> There may be an argument for recognising that where an organisation is delivering a health service and there is a stated legal authority for it to collect health information about an individual, NPP 10 should permit this to occur without consent.[172]

8.156 The OPC Review recommended that:

> The Australian Government should consider amending NPP 10.2 to permit the collection of health information (under NPP 10.2(b)(i)) 'as authorised by law' in addition to 'as required by law'.[173]

8.157 Section 2 of the *Privacy Legislation Amendment Act 2006* (Cth) amended NPP 10.2(b)(i) to read 'as required or authorised by or under law'.

8.158 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 OPC

---

170 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 3.

171 See, eg, *Public Health Act 1991* (NSW) s 14; *Health (Infectious Diseases) Regulations 2001* (Vic) reg 6.

172 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 278.

173 Ibid, Rec 83.

Review noted that the exact nature and construction of these binding rules is uncertain. The OPC was not aware of any examples of rules that would satisfy the requirements of NPP 10.2(b)(ii).[174] The draft *National Health Privacy Code* does not include this exception in NHPP 1.

8.159 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.[175]

8.160 Another difficulty arises from the interaction of NPP 2 on use and disclosure and NPP 10 on collection. In any communication of health information, there is both a disclosure and a collection. For example, a health service provider's disclosure of health information to an insurance company following an adverse medical event may be permitted by NPP 2. The disclosure is directly related to the primary purpose and is likely to have been within the reasonable expectation of the individual. NPP 10, however, does not appear to allow collection by the insurance company in the same circumstances. It is unclear whether NPP 10.1(e)—that the collection is necessary for the establishment, exercise or defence of a legal or equitable claim—would cover the early reporting of an adverse incident where there is not and may never be a legal claim.

Question 8–15 Should NPP 10 of the *Privacy Act* be amended to clarify when health information may be collected without consent? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of health information without consent?

Question 8–16 Are there any other issues relating to the collection of health information that the ALRC should consider?

Use and disclosure of health information

8.161 IPPs 10 and 11 and NPP 2 regulate the use and disclosure of personal information. IPPs 10 and 11 provide 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

174 Ibid, 279.
175 Ibid, Rec 84.

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.[176]

8.162 NPP 2 provides that 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.

8.163 Concern was expressed in the course of the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act* (Senate Committee privacy inquiry)[177] and the OPC Review[178] that the concept of 'primary purpose of collection' may be interpreted in a narrow way and that it might impede the provision of holistic health care and the appropriate management of an individual's health.

8.164 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'.

8.165 The AMA also notes 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 future health and well being. Health care is an on-going process that spans from conception through to death.[179]

---

176 The *Privacy Legislation Amendment Act 2006* (Cth), passed in September 2006, amended NPP 2.1 to allow 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 a genetic relative's life, health or safety, but not necessarily an imminent threat. This amendment is intended to implement, in part, Rec 21–1 of ALRC 96. Any such use or disclosure will have to be done in accordance with guidelines relating to the use and disclosure of genetic information. Under new section 95AA the guidelines will be issued by the National Health and Medical Research Council and approved by the Privacy Commissioner.

177 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [5.63].

178 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.

179 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.

8.166 Under the NPPs, the 'primary purpose of collection', however, is linked to the express and implied consent of the health consumer and may not be something that can be defined in advance for every health consumer in every situation. The OPC Guidelines state in relation to NPP 2 that the 'primary purpose' 'is the main or dominant reason a health service provider collects information from an individual'.[180]

8.167 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.[181]

8.168 The OPC Review recommended that:

> The Office will 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 health care.[182]
>
> The Office will provide clearer guidance on the operation of NPP 2 to give more effective and practical assistance to demonstrate how the principle operates. This will take into account the range of relationships between health services and individuals, particularly where individuals agree to a holistic approach to the delivery of a health service.[183]

8.169 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.

---

180 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline 2.1.

181 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 263.

182 Ibid, Rec 77.

183 Ibid, Rec 78.

8.170 This provision provides scope for the use of health information outside a particular episode of care and without the consent of the health consumer. For example, it would allow health service providers to refer to their existing records about an individual.

8.171 The ALRC is interested in hearing whether these issues require further consideration in the course of the ALRC's Inquiry and whether NHPP 2 provides a more appropriate and effective framework for the use and disclosure of health information than the current provisions of the *Privacy Act*.

Question 8–17 Is guidance by the Office of the Privacy Commissioner an appropriate and effective response to concerns that the phrases in NPP 2, 'primary purpose of collection' and 'directly related to the primary purpose', might impede the appropriate management of an individual's health? If not, what is an appropriate and effective response?

Question 8–18 Does NHPP 2 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for the use and disclosure of health information than the current provisions of the *Privacy Act*?

Question 8–19 Are there any other issues relating to the use and disclosure of health information that the ALRC should consider?

Access to health information

8.172 In *Breen v Williams*,[184] the High Court of Australia unanimously held that health consumers do not have a right of access to their medical records at common law. Health consumers must therefore rely on legislation, including the *Privacy Act*, to allow them a right of access to their medical records.

8.173 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.

8.174 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 *Freedom of Information Act* and the *Archives Act 1983* (Cth). Chapter

184 *Breen v Williams* (1996) 186 CLR 71.

4 addresses the issue of whether IPP 6 should set out more clearly the circumstances in which agencies can deny an individual access to his or her personal information, including health information.

8.175 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.[185] The list of exceptions also includes situations in which denying access is required or authorised by or under law.[186]

8.176 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, 163 concerned a refusal of access to health records.[187] In the course of the OPC Review the Australian Privacy Foundation expressed the view that organisations should be required to give access to as much information as possible, even when an exception applies to some information.[188]

8.177 Both 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.[189]

8.178 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.[190]

8.179 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 expressly address 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:

---

185 *Privacy Act 1988* (Cth) sch 3, NPP 6.1(b).
186 Ibid sch 3, NPP 6.1(h).
187 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 112.
188 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.
189 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 115.
190 Ibid, 117.

> The Office will develop further guidance on the operation of NPP 6.1 on 'serious threat to life or health', explaining that a serious threat to a therapeutic relationship could be a serious threat to a person's health. This will go some way towards addressing what appears to be a too narrow interpretation of NPP 6.1(b) by some practitioners.[191]

8.180 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. The grounds provided in NHPP 6 for refusing access, however, are essentially the same as those provided in NPP 6. NHPP 6 provides in addition 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.[192]

8.181 The draft Code also sets out detailed provisions in relation to the possible forms of access. For example, a right of access may be exercised by inspecting the health information—or by inspecting a printout of the information if the information is in electronic form—and having the opportunity to take notes of the contents; by receiving a copy of the information; by viewing the health information and having the content explained by the health service provider who holds the information or another suitably qualified individual.[193]

8.182 The ALRC would be interested in hearing whether the exception in NPP 6.1(b) in relation to providing access to health information—that is, that access may be denied if it would pose a serious threat to the life or health of any person—is appropriate. Should the exception be extended to allow a health service provider to deny access to health information if doing so would pose a threat to the therapeutic relationship between the health service provider and the health consumer?

Question 8–20 Is the exception in NPP 6.1(b) in relation to providing access to health information (that is, that access may be denied if it would pose a serious threat to the life or health of any person) appropriate and effective? Should the exception 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?

---

191 Ibid, Rec 30.

192 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003), NHPP 6.1.

193 Ibid pt 5 div 1 s 2.

Use of intermediaries

8.183 The IPPs do not provide a mechanism for dealing with the situation in which access to information is refused. A consumer refused access to health information by an agency could, however, lodge a complaint with the Privacy Commissioner under s 36 of the *Privacy Act*.

8.184 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.

8.185 The OPC Review noted that this right is a very limited one.[194] Organisations are only required to consider whether the use of an intermediary would meet the needs of the parties but is 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 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.

8.186 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.[195]

8.187 The OPC expressed the view that, while these prescriptive and detailed provisions would not be suitable for inclusion in the NPPs, the NPPs could include a similar right to the use of an intermediary. The OPC also noted that if the draft *National Health Privacy Code* became a schedule to the *Privacy Act*—in accordance with Recommendation 29 of the OPC Review—the matter would then be addressed.[196]

---

194 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 117.

195 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 5 div 3.

196 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 117.

Fees for access

8.188 NPP 6.4 provides that 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.

8.189 In its submission to the OPC Review, the Australian Privacy Foundation expressed the view that, while this provision seemed appropriate, the OPC's assessment of 'excessive' in some cases was not reasonable.[197] This issue is not limited to fees for access to health information and the issue is addressed generally in Chapter 4.

8.190 The draft *National Health Privacy Code* includes provision for maximum fees for access to health information to be prescribed by regulation.[198] The detailed provisions contained in the draft Code dealing with the way a right of access might be exercised, discussed above, may provide a more comprehensive basis for the calculation of appropriate maximum fees.

8.191 The OPC noted in response to concerns about excessive fees that the Australian Government could introduce a table of recommended fees in a schedule to the *Privacy Act*.[199] The OPC recommended that:

> The Australian Government should consider adopting the Australian Health Ministers' Advisory Council (AHMAC) Code as a schedule to the Privacy Act (see also recommendations 13, 33 and 35). This will address the issue of intermediaries, and the issue of fees for access.[200]
>
> The Office will develop guidance on fees for access to personal information.[201]

Health service provider is sold, transferred or closed

8.192 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.[202] 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

---

197 Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004.

198 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) pt 5 div 1 cl 6(2)(a).

199 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 118.

200 Ibid, Rec 29.

201 Ibid, Rec 31.

202 Ibid, 123.

practitioner taking over the practice or that they are provided to the patient to whom they relate.[203]

8.193 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.[204]

8.194 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.

8.195 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.[205] It is also important to ensure that health information is available to health consumers seeking health services in the future.

8.196 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.)[206]
>
> 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.[207]

8.197 The ALRC is interested in views in relation to these issues.

Question 8–21 Do NHPP 6 and Part 5 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for access to health information than the current provisions of the *Privacy Act*?

---

203 *Medical Practice Regulation 2003* (NSW) reg 8.
204 *Health Records Act 2001* (Vic) s 19, HPP 10.
205 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 123.
206 Ibid, Rec 35.
207 Ibid, Rec 36.

Question 8–22 Should the *Privacy Act* be amended to deal expressly with the situation in which a health service provider ceases to operate? Does NHPP 10 of the draft *National Health Privacy Code* provide an appropriate and effective framework to deal with this situation?

Question 8–23 Are there any other issues the ALRC should consider in relation to access to health information?

Transfer of health information

8.198 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 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.

8.199 The OPC Review recommended that:

> The Australian Government should consider adopting the Australian Health Ministers' Advisory Council (AHMAC) code as a schedule to the Privacy Act. This will address the issue of the transfer of health records to another health service provider. (See also recommendations 13, 29 and 35.)[208]
>
> 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 11 in the AHMAC Code.[209]

8.200 The ALRC is interested in views in relation to this issue.

Question 8–24 Does NHPP 11 of the draft *National Health Privacy Code* provide a more appropriate and effective framework to deal with the transfer of health information from one health service provider to another than the current provisions of the *Privacy Act*?

208 Ibid, Rec 33.
209 Ibid, Rec 34.

Health and medical research

8.201 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.[210]

8.202 There is strong community support for health and medical research. Over 90% of voters in an AC Neilson survey conducted for Research Australia in 2003 thought that investing in health and medical research was important or very important. These voters ranked health and medical research as the third highest priority for government funding after healthcare and education.[211]

8.203 The NHMRC is a statutory authority established by the *National Health and Medical Research Council Act 1992* (Cth) (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.[212]

8.204 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 funding of health and medical research is primarily provided from the Medical Research and Endowment Account established under the NHMRC Act.[213] 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

---

210 Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle For a Healthy Competitive Australia* (2004), Minister's Forward.
211 Ibid, 20.
212 *National Health and Medical Research Council Act 1992* (Cth) s 3.
213 Ibid pt 7.

in health and medical research since 1999 and that funding in 2004–05 was more than $420 million.[214]

8.205 The final report of 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.[215]

8.206 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 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.[216]

8.207 The NHMRC noted in its submission to 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.[217]

8.208 Under the NHMRC Act, AHEC—a principal committee of the NHMRC—has responsibility for developing guidelines for the ethical conduct of medical research.[218] The primary guideline developed by AHEC for this purpose is the *National Statement on Ethical Conduct in Research Involving Humans*[219] (National Statement). The National Statement sets out ethical principles relevant to research involving humans and guidance on the formation, membership and functions of HRECs.

---

214 National Health and Medical Research Council, *Role of the NHMRC* <www.nhmrc.gov.au/about/role/index.htm> at 10 August 2006.

215 Investment Review of Health and Medical Research Committee, *Sustaining the Virtuous Cycle For a Healthy Competitive Australia* (2004), 17.

216 Ibid, 17.

217 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.

218 *National Health and Medical Research Council Act 1992* (Cth) s 35(3).

219 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999). The National Statement is currently under review and a second round of public consultation was conducted in the first quarter of 2006.

8.209 The National Statement provides that research proposals involving human 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.

8.210 Despite the fact that the National Statement does not have the force of law, there is a high level of voluntary compliance. Compliance with the National Statement is a condition of NHMRC grants of research funds.[220]

8.211 As discussed below, the *Privacy Act* regime incorporates the HREC approval process established by the National Statement to ensure that research is conducted with due regard for the protection of personal health information.

Consent

8.212 The conduct of health and medical research frequently involves the collection and use of health information about individuals. Generally, individuals who participate in health or medical research projects do so on the basis of consent and, in these circumstances, it is possible to handle participants' health information in compliance with the IPPs or the NPPs. The National Statement makes clear that:

> Before research is undertaken, whether involving individuals or collectivities, the consent of the participants must be obtained, except in specific circumstances defined elsewhere in the Statement.
>
> The ethical and legal requirements of consent have two aspects: the provision of information and the capacity to make a voluntary choice. So as to conform with ethical and legal requirements, obtaining consent should involve:
>
> (a) provision to participants, at their level of comprehension, of information about the purpose, methods, demands, risks, inconveniences, discomforts, and possible outcomes of the research (including the likelihood and form of publication of research results); and
>
> (b) the exercise of voluntary choice to participate.[221]

---

220 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. However, as noted above, 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.

221 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), [1.7]. See also the detailed discussion of consent—including consent to unspecified future research—in Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Ch 15.

8.213 The *Privacy Act*, 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. The Act provides a mechanism to allow such research to go forward subject to guidelines issued by the NHMRC and approved by the Privacy Commissioner.

8.214 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 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

8.215 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.

8.216 The current *Guidelines under Section 95 of the Privacy Act 1988*[222] (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

222 National Health and Medical Research Council, *Guidelines under Section 95 of the Privacy Act 1988* (2000).

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

8.217 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:

- the purpose cannot be served by the collection of information that does not identify the individual;[223]
- it is impracticable for the organisation to seek the individual's consent to the collection, use or disclosure;[224]
- the information is collected, used and disclosed in accordance with guidelines approved under s 95A;[225]
- 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;[226] and
- the organisation takes reasonable steps to de-identify permanently the information before it discloses it.[227]

8.218 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*[228] (Section 95A Guidelines) were issued in 2001.

Sections 95 and 95A Guidelines

8.219 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' health information. In particular, HRECs must consider, and may approve, research proposals seeking to use identifiable health information without consent. HRECs may approve such research proposals 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.

---

223 *Privacy Act 1988* (Cth) sch 3, NPP 10.3(b).
224 Ibid sch 3, NPPs 2.1(d)(i), 10.3(c).
225 Ibid sch 3, NPPs 2.1(d)(ii), 10.3(d).
226 Ibid sch 3, NPP 2.1(d)(iii).
227 Ibid sch 3, NPP 10.4.
228 National Health and Medical Research Council, *Guidelines Approved under Section 95A of the Privacy Act 1988* (2001).

8.220 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 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.[229] However, these organisations may be covered by state legislation.[230]

8.221 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.[231] The NHMRC expressed the view that this was hindering the conduct of effective health and medical research.[232]

8.222 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.[233] In response, the OPC Review stated that 'the *Privacy Act* is not intended to restrict important medical research'[234] 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.[235]

8.223 The draft *National Health Privacy 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—

---

229 *Privacy Act 1988* (Cth) s 6C.

230 See, eg, *Health Records Act 2001* (Vic) HPPs 1.1(e)(iii), 2.2(g)(iii).

231 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 201.

232 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.

233 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.

234 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 199.

235 Ibid, Rec 62 (in part).

> … if the collection is necessary for research, or the compilation or analysis of statistics, in the public interest—
>
> (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.[236]

8.224 NHPP 2 provides similar criteria for the use and disclosure of health information for research with some additional safeguards around disclosure.[237] The revised draft Code also includes draft mandatory guidelines for research.[238] As noted above, the 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, and in every Australian state and territory, including in the field of health and medical research.

8.225 The issues of complexity, fragmentation and inconsistency in the privacy regime are discussed in general terms in Chapters 2, 4 and 7 of this Issues Paper. Chapter 2 examines the options for a nationally consistent privacy regime. Chapter 4 examines the need for a single set of privacy principles. Chapter 7 examines a range of issues such as multiple regulators and the complexity of interactions between federal, state and territory laws. The first part of this chapter examines the need for a nationally consistent regime for handling health information, including in the context of health and medical research. A nationally consistent privacy regime, a single set of privacy principles or a nationally consistent regime for the handling of health information would eliminate the need for two sets of Guidelines. The ALRC does not, therefore, propose to examine separately the need for a single set of Guidelines—that question is subsumed in the higher level questions posed in other parts of this Issues Paper.

8.226 The following sections examine some of the fundamental elements of the regime that currently regulates the use of health information in health and medical research and seek views on whether these elements are appropriate and effective.

The public interest balance

8.227 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:

---

236 National Health Privacy Working Group of the Australian Health Ministers' Advisory Council, *Draft National Health Privacy Code* (2003) sch 1, NHPP 1.1(e).

237 Ibid sch 1, NHPP 2.2(g).

238 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 65.

> 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.[239]

8.228 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.

8.229 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.[240] In considering the public interest balance, HRECs are required to consider certain specified matters including:

- 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.

8.230 A number of the submissions to the OPC Review expressed the view that the *Privacy Act* and the 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

---

239 Commonwealth, *Parliamentary Debates*, House of Representatives, 12 April 2000, 15749 (D Williams—Attorney-General).

240 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.

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.[241]

8.231 Dr Gun also states that:

> Rulings such as this suggest that we researchers are not to be trusted to protect privacy; that names will be released to outside parties; or that publications will identify individuals. This might be justified if there were some evidence that researchers have actually misused such data. Yet where is such evidence? The fact that there is no evidence of misuse is easily explained: researchers have nothing to gain by providing information and everything to lose. I know that if it became known that confidential information had been given out from my research team, it would be the end of my research and my career.[242]

8.232 The NHMRC considers that

> an appropriate balance between individual privacy and the public interest in the provision of quality health care and the conduct of effective health and medical research is not being achieved within the current federal privacy framework.[243]

8.233 The Australian Compliance Institute suggested that special provision should be made in relation to the use of health information for research that will benefit the government, environment and community. The Institute also was of the view that the Privacy Commissioner should have the power to exempt research of this nature from the *Privacy Act*.[244]

8.234 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.[245]

---

241 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.

242 Ibid.

243 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.

244 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.

245 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 210.

8.235 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 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.[246]

8.236 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.[247]

8.237 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.[248] 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.[249]

8.238 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.[250] It would also be possible to raise

---

246 Ibid, 211.

247 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.

248 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.

249 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.

250 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.

awareness about the application of the *Privacy Act* and the Section 95 and 95A Guidelines in the research context.

8.239 NHPP 1 of the draft *National Health Privacy Code* provides that research must be in the public interest in order for it to proceed in accordance with guidelines issued for the purpose. The public interest in the research would not have to 'substantially outweigh' the public interest in the protection of privacy, but any research would have to be conducted in accordance with guidelines.

8.240 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, and the public interest in protecting individuals' privacy (including individuals having choices about the use of their information for such research purposes).[251]

8.241 The OPC noted that some of the issues to be considered in this context were: whether additional privacy principles or guidelines would be necessary if the balance was shifted to allow greater access to health information without consent by health and medical researchers; and whether special considerations arise where research is conducted for commercial purposes.

8.242 The ALRC would be interesting in views on whether the test provided in the *Privacy Act* and Section 95 and 95A Guidelines—that the public interest in research must substantially outweigh the public interest in the level of privacy protection provided by the Act—is too strict. Does the test achieve an appropriate balance between the interests of promoting health and medical research in the public interest and protecting individual's privacy and, if not, where should the balance lie?

Question 8–25 Is the current public interest test in the *Privacy Act* and Section 95 and Section 95A Guidelines (that the public interest in promoting research substantially outweighs the public interest in maintaining the level of protection of health information provided by the Act) appropriate and effective? If not, what is an appropriate and effective test?

Definition of research

8.243 Section 6 of the *Privacy Act* states that '*medical research* includes epidemiological research', but the term is not otherwise defined. The NHMRC notes that:

---

251 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.

> It is unclear whether the term 'medical research' includes, for example, nursing, psychological, sociological or health services research, all of which are extremely important to the ongoing efficiency and effectiveness of our health care system.[252]

8.244 The IPPs do not refer to health or medical research, but s 95 of the *Privacy Act*[253]—which provides for the development of the Section 95 Guidelines—refers to 'medical research'.

8.245 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 is relevant to public health or public safety to bring the research within the regime established by the NPPs and the Section 95A Guidelines. The NHMRC notes that:

> There is also no readily available legislative definition of the term 'public health and public safety' which is critical to the operation of Section 95A. The term suggests a requirement of relevance to a sector of the community which is broader than a few individuals. It is possible that organisations may seek to conduct research that involves the collection, use or disclosure of health information which is relevant only to a few individuals, rather than to a broad sector of the community, but nevertheless is of scientific importance and ethically robust. The Privacy Act does not appear to enable such research by organisations, even if it is strongly in the public interest, if its conduct requires the collection, use or disclosure of health information without consent.[254]

8.246 In addition, the NHMRC states 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.

8.247 The National Statement points out that there are many definitions of research and that it remains difficult to find a single agreed definition.[255] The National Statement is, however, currently under review and the second consultation draft of the *National Statement on Ethical Conduct in Human Research* defines research as follows:

> Research is to be understood as including investigation undertaken in order to gain knowledge and understanding or in order to train researchers, and the use of existing knowledge in experimental development to produce new or substantially improved materials, devices, products and processes. It does not include routine testing and routine analysis of materials, components and processes as distinct from the development of new analytical techniques. However, some of these activities, such as

---

252 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.

253 Section 73 of the *Privacy Act*, which deals with applications for Public Interest Determinations by the NHMRC, also refers to 'medical research'.

254 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.

255 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), 7.

> quality assurance, may sometimes warrant ethical review, even though they are not research.[256]

8.248 The AMA submission to the OPC Review suggested that all medical research should be considered relevant to public health and safety.[257] The NHMRC recommended that the regime provided in s 95 of the *Privacy Act* and the NPPs should apply to all health and medical research and noted that the term should be used consistently throughout the Act.[258]

8.249 Chapter 4 addresses the question of whether 'research' for the purposes of the *Privacy Act* should include research involving non-health information. The ALRC is interested in views on whether the term 'research' should be defined for the purposes of the *Privacy Act*. This definition will be important particularly if, for example, there is to be any shift in the public interest balance between the protection of individual privacy and the conduct of health and medical research in the future.

Question 8–26 Should the term 'research' be defined for the purposes of the *Privacy Act*? If so, how should the term be defined?

Identifiable health information

8.250 '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.[259]

8.251 The OPC Guidelines indicate that the *Privacy Act* does not apply to 'de-identified information or statistical data sets, which would not allow individuals to be identified'.[260] 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

256 National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, *National Statement on Ethical Conduct in Human Research: Second Consultation Draft* (2006).

257 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.

258 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.

259 *Privacy Act 1988* (Cth) s 6.

260 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), Guideline A.3.1.

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.[261]

8.252 The OPC Review identified a number of problems with this concept. 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 clarify this phrase so that it is clear when information is not subject to the *Privacy Act* or the HREC approval process.[262] The Australian Institute of Health and Welfare also pointed to problems with determining when data is de-identified and indicated that there is a need for more guidance.[263] 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.*[264]

8.253 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.[265]

8.254 The National Statement makes a distinction between identified, potentially identifiable (coded or re-identifiable) and de-identified (not re-identifiable or anonymous) personal information.[266] These categories have been reconsidered in developing the second consultation draft of the National Statement, which provides as follows:

> Data are collected, stored or disclosed, as identifiable data, re-identifiable or potentially identifiable data, or non-identifiable data (which includes a subset, anonymous data). These three categories of data, described below, are mutually exclusive:

---

261 Office of the Privacy Commissioner, 'De-identification of Personal Information', (Paper presented at Privacy Contact Officers Network Meeting, Canberra, 26 November 2004).

262 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.

263 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.

264 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.

265 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.

266 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), 9.

> - individually identifiable: data from which the identity of a specific individual can reasonably be ascertained. Examples of identifiers may include the individual's name, image, date of birth or address;
> - re-identifiable or potentially re-identifiable: data from which identifiers have been removed and replaced by a code, but from which it remains possible to re-identify a specific individual, for example, by using the code or by linking different data sets;
> - non-identifiable: data that 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. This includes a subset, anonymous: data which can be linked with other data so it can be known that they are about the same data subject, while the identity of that specific individual remains unknown.
>
> The term 'de-identified data' sometimes refers to a record that cannot be linked to an individual (non-identifiable), and at other times refers to a record in which identifying information has been removed but for which the means exist to re-identify the individual (re-identifiable or potentially re-identifiable). Because of this ambiguity, the terms above are preferred. When the term 'de-identified data' is used, researchers and those reviewing research need to establish precisely which of these possible meanings it has. It should be noted that with advances in genetic knowledge and data linkage, and the proliferation of tissue banks of identified material, human tissue samples may always be regarded as, in principle, potentially re-identifiable.[267]

8.255 Where health information is 'non-identifiable', use of the information would fall outside the protection of the *Privacy Act*. However, where health information is 'identifiable' the *Privacy Act* and the Section 95 and 95A Guidelines clearly require HREC privacy approval. The situation is more complex in relation to 're-identifiable' information. Is health information 'de-identified' for the purposes of the *Privacy Act* where it has been coded, an independent intermediary holds the code, and it is not possible for researchers to ascertain the identity of the individuals concerned without the assistance of the intermediary? This may depend on the arrangements established between the researchers and the intermediary.

8.256 The ALRC would be interested in views about whether the definitions of 'identifiable', 're-identifiable' and 'non-identifiable' set out in the second consultation draft of the National Statement are appropriate for inclusion in the *Privacy Act*.

8.257 In addition, the ALRC would be interested in views on whether 'identifiable' and 're-identifiable' or coded health information should be treated in the same way in the context of health and medical research. Associate Professor Roger Magnusson has suggested, for example, that the use of Unique Patient Identifiers for Research may provide a basis for broad yet privacy-sensitive access to health information for research

---

267 National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, *National Statement on Ethical Conduct in Human Research: Second Consultation Draft* (2006), 25–26.

purposes. This approach would build on initiatives discussed above in relation to the use of Individual Healthcare Identifiers.[268]

8.258 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.[269] 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 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.[270]

Question 8–27 Should the *Privacy Act* be amended to include definitions of 'identifiable', 're-identifiable' and 'non-identifiable' personal information?

Question 8–28 Should the *Privacy Act* draw a distinction between 'identifiable' and 're-identifiable' health information in the context of health and medical research?

Impracticable to seek consent

8.259 NPP 2 allows the 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 use or disclosure. The Section 95 Guidelines allow the use and disclosure of health information by agencies without consent when it is reasonable for the research to proceed without this consent.

8.260 In its submission to the OPC Review, the NHMRC noted the inconsistency between NPP 2 and the National Statement in relation to the use and disclosure of health information in epidemiological research without consent. The National Statement states that epidemiological research

---

268 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 53.

269 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].

270 Ibid, Rec 18–3.

> is concerned with the description of health and welfare in populations through the collection of data related to health and the frequency, distribution and determinants of disease in populations with the goal of improving health.[271]

8.261 The National Statement recognises that some epidemiological research may require whole population studies. The National Statement makes clear that consent of participants generally should be obtained for the use of identifiable or potentially identifiable data for epidemiological research.[272] However, an HREC may approve access to such data without consent where it is satisfied that: it is 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 are likely either to cause unnecessary anxiety for those whose consent would be sought or to prejudice the scientific value of the research; and the public interest in the research outweighs to a substantial degree the public interest in privacy.[273]

8.262 The OPC Review noted evidence that requiring an opt-in approach to participation in some research projects significantly reduces the participation rate—and therefore the scientific value and integrity of the research.[274]

8.263 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.[275] A number of other submissions to the OPC Review expressed the view that the circumstances in which NPP 2 allows the use and disclosure of health information without consent are too narrow.[276]

8.264 The second consultation draft of the National Statement provides detailed provisions relating to consent, including provisions dealing with the qualifying or waiving of consent requirements in some circumstances. The draft National Statement states that HRECs may waive the requirement for consent if satisfied that:

---

271 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), 40.

272 Ibid, [14.3].

273 Ibid, [14.4].

274 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 211.

275 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.

276 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.

(a) participation in the research involves no more than low risk to participants;

(b) it is impracticable to obtain consent;

(c) there is a sufficient justification for the waiver;

(d) the research could not practicably be carried out without the waiver;

(e) any risks to the privacy of participants will be minimised;

(f) there is an adequate plan for contacting participants with information derived from the research, should the need arise;

(g) whenever appropriate, the participants will be provided with additional pertinent information after participating;

(h) the benefits from the knowledge to be gained from the research justify any risks of harm associated with not seeking consent; and that

(i) the waiver is not otherwise prohibited by State, federal, or international law.[277]

8.265 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).[278]

8.266 The ALRC remains of the view that the National Statement and the *Privacy Act* should be consistent as far as possible. The ALRC is interested in views on: what provision should be made for the use of health information without consent in health and medical research; and whether the test in NPP 2 that information may be used where it is impracticable to seek consent is appropriate and effective.

Question 8–29 What provision should be made for the use of health information without consent in health and medical research?

Question 8–30 Does NPP 2 provide an appropriate and effective framework for the use, without consent, of health information in health and medical research?

277 National Health and Medical Research Council, Australian Research Council and Australian Vice-Chancellors' Committee, *National Statement on Ethical Conduct in Human Research: Second Consultation Draft* (2006), [2.2.22].

278 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.

Human Research Ethics Committees

8.267 The NHMRC National Statement requires that every research proposal involving humans must be reviewed by an HREC and must not be undertaken or funded unless approval has been granted. Institutions and organisations that undertake research involving humans must establish individually or jointly, adequately resource and maintain an HREC composed and functioning in accordance with the National Statement.[279] The primary role of an HREC is to protect the welfare and the rights of participants in research.[280]

8.268 The minimum membership of an HREC is seven, comprising: a chairperson; at least two community members, one man and one woman, who have no affiliation with the institution or organisation; at least one member with current knowledge and experience in the relevant area of research; at least one member with current knowledge and experience in professional care, counselling or treatment; at least one member who is a minister of religion or a person who performs a similar role in a community (such as an Aboriginal elder); and at least one lawyer.[281]

8.269 Both the Section 95 and 95A Guidelines require that, before making a decision under the Guidelines, 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.[282] The Section 95A Guidelines note that it may be necessary to appoint additional members with specific expertise in some circumstances.

8.270 A number of issues in the privacy area were identified in the course of the OPC Review relating to decision making by HRECs. Dr Gun expressed the view that HRECs have a tendency to make what he characterised as conservative decisions, refusing access to health information if there is any risk of being in breach of the law.[283] In addition, he noted that it is often necessary to involve a number of HRECs in decision making in relation to research proposals, particularly national proposals.[284] Concern was also expressed about inconsistencies in the way HRECs balance the public interests in research and privacy,[285] and in relation to membership of HRECs.[286]

---

279 National Health and Medical Research Council, *National Statement on Ethical Conduct in Research Involving Humans* (1999), [2.1].

280 Ibid, [2.5].

281 There may be overlapping of the categories, for example, the chair may also be a lawyer.

282 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].

283 NHMRC Privacy Working Committee, *Consultation PC 13*, Canberra, 30 March 2006 made a similar point.

284 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.

285 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.

8.271 ALRC 96 considered in detail the role and function of HRECs in the particular context of genetic research, and made a range of recommendations to improve HREC decision making and to support HRECs in their work. 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.[287]

8.272 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.[288]

8.273 A quality improvement program targeting the elements set out in Recommendation 17–1, above—in particular consolidation of ethical review by subject-matter; the membership and need for particular expertise of HRECs; education and training of HREC members; and standardised record keeping and reporting arrangements to the NHMRC—also could target HREC decision making on privacy.

8.274 Given this recent comprehensive review, the ALRC does not propose to reconsider the HREC decision-making process in detail. The ALRC would, however,

---

286 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.

287 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.

288 Ibid, Rec 15–3.

be interested in views on the threshold issue of whether HRECs are the most appropriate bodies to make decisions about the collection, use and disclosure of health information without consent in the context of health and medical research.

8.275 In addition, the ALRC would be interested in views on whether the requirements imposed on HRECs by the Section 95 and 95A Guidelines are appropriate and effective. 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.[289]

8.276 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.[290]

Question 8–31 Are Human Research Ethics Committees 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?

Question 8–32 Are the requirements imposed on Human Research Ethics Committees by the Section 95 and Section 95A Guidelines issued under the *Privacy Act* appropriate and effective?

Health databases and data linkage

8.277 Health databases may be established for a number of reasons in both the health services and the health and medical research contexts. As noted above, the Australian Government maintains the Medicare and Pharmaceutical Benefits Program databases. State and territory governments in Australia have established a range of 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.[291]

---

289 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.

290 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.

291 *Public Health Act 1991* (NSW) s 42G.

8.278 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.[292] 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 donated by volunteers specifically for the Centre's research projects.

8.279 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.

8.280 Associate Professor Roger Magnusson has noted that:

> The regulation of research claims to health data is a pressing issue that will become increasingly important in future. On the one hand, the trend in health privacy protection is towards an increasingly complex, and constraining, web of legislation. This creates logistical and compliance problems for researchers, and others contributing to the development of health data assets … On the other hand, 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 within the degenerative diseases that increasingly account for morbidity and mortality, 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.[293]

8.281 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.

8.282 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 expectation of health consumers. The NHMRC noted that getting consent from all 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.

---

292 ANZDATA is located at The Queen Elizabeth Hospital in South Australia.

293 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 8.

8.283 The NHMRC noted that, on this basis, such registers would appear to require approval by an HREC, according to the Section 95A Guidelines. It would be extremely difficult, however, 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 protects appropriately the public interest.[294]

8.284 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 predate the development of a formal research proposal and 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*.

8.285 Data registers also raise the issue of data linkage. Identifying and investigating the relationships between risk factors and disease frequently require researchers to match accurately data relating to the same individual. Associate Professor Magnusson notes the emerging body of literature highlighting the need for researchers, especially epidemiologists, to have access to identifying information for the purposes of data linkage studies.[295] The NHMRC noted, however, that some HRECs appear to reject research proposals automatically where they involve data linkage of health information without consent, apparently in the 'mistaken belief that such linkage is not ethically or legally acceptable'.[296]

8.286 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

294 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 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.

295 R Magnusson, 'Data Linkage, Health Research and Privacy: Regulating Data Flows in Australia's Health Information System' (2002) 24 *Sydney Law Review* 5, 10.

296 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.

chapter or otherwise) should include specific guidance on obtaining consent to unspecified future research.[297]

8.287 The ALRC would be interested in views on whether the *Privacy Act* provides an appropriate and effective regime for the establishment, maintenance and use of health data registers.

Question 8–33 Does the *Privacy Act* provide an appropriate and effective regime for: (a) the establishment of health data registers; and (b) the inclusion and linkage of health information in data registers?

297 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.

9. Children, Young People and Adults with a Decision-Making Disability

Contents

Introduction

9.1 This chapter will consider existing laws and practices applying to privacy of children and young people, including recognition at international law of the right of children to privacy and how the *Privacy Act 1988* (Cth) and other Australian legislation relates to children and young people. The issue of decision-making capacity is a key factor that arises in this discussion, although the chapter considers other issues that may arise in relation to the privacy of children and young people.

9.2 The chapter also looks at adults with a decision-making disability and whether there is a need to change the *Privacy Act* or other legislation to facilitate better the protection of the personal information of this group.

Privacy of children and young people

9.3 Privacy of children and young people has not received a great deal of attention and discussion as a separate issue in Australia. Of particular note is the discussion of children's privacy which occurred at the time of passage of the *Privacy Amendment (Private Sector) 2000 Act* (Cth). Labor moved amendments that would require a commercial service to obtain the consent of a child's parent before collecting, using or disclosing personal information from a child aged 13 or under.[1] While the amendment was not agreed to by the Government, it was indicated that the issue would be investigated further.[2]

9.4 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]

9.5 Children's privacy was specifically exempted 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 (OPC Review).[5] The 2005 review of the *Privacy Act* by the Senate Legal and Constitutional References Committee did not examine children's privacy as a separate issue and made no recommendations on the issue.[6] The Terms of Reference for this Inquiry do not exclude children's privacy, and the ALRC will be considering it as part of this broader Inquiry.

9.6 This chapter examines some particular areas of practice where children most often intersect with the law, namely child welfare, juvenile justice and family law, and the privacy issues that arise in those areas. The chapter also looks at some particular

---

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 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 3 May 2006.

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).

issues that raise questions about the privacy of children and young people, such as: disclosure of health information to parents; information held by schools and child care centres; online consumer information; taking and publishing photographs; broadcasting of identifying images and information; and identification in court records. As noted in Chapter 1, the issue of credit reporting will be dealt with in a separate Issues Paper to be published later in 2006, and will include consideration of the impact of credit reporting on children and young people.

9.7 Chapter 1 sets out a number of issues which will not be dealt with in this Inquiry, either because they fall outside the scope of the Terms of Reference or they are already under consideration by another body or adequately covered by existing regulation. There are a number of issues often associated with children's privacy which will not be dealt with this by the Inquiry.

- **Organ and tissue donation.** There are a number of ethical issues surrounding decisions made by parents or guardians to allow (or require) a child or young person to be an organ or tissue donor. As noted in Chapter 1, this Inquiry will not be considering privacy relating to intrusions of the physical body.

- **Consent to medical treatment.** Issues relating to consent to medical treatment for children and young people, and whether the consent can be given by the child or young person, a parent or another person or body, are issues of privacy of the body and will not be dealt with in this Inquiry. This Inquiry will, however, consider disclosure of and access to children's and young people's medical information. All of these issues also are the subjects of a current inquiry by the New South Wales Law Reform Commission.[7]

- **Drug or genetic testing.** Drug testing of children and young people, particularly in a school environment, is an issue of concern to many. This has been excluded from this Inquiry as it is privacy relating to invasion of the body. A number of issues related to genetic testing of children and young people were dealt with by the ALRC and the Australian Health Ethics Committee in the report *Essentially Yours: The Protection of Human Genetic Information* (ALRC 96, 2003).

- **Newborn screening cards.** Commonly known as 'Guthrie cards', newborn screening cards contain a small sample of blood taken between two and five days after birth and the personal details of virtually all children born in Australia. The blood is tested for a range of congenital diseases. Concerns have been raised about the lack of understanding of the tests, the lack of informed consent and the way in which the cards are stored and could be used in the

7 New South Wales Law Reform Commission, *Minors' Consent to Medical Treatment*, IP 24 (2004). A final report is expected in 2007.

future.[8] The ALRC and Australian Health Ethics Committee considered newborn screening cards in the report *Essentially Yours: The Protection of Human Genetic Information* (ALRC 96, 2003).[9] Although the ALRC does not intend to revisit this specific issue as part of this Inquiry, the protection of health information is generally considered in Chapter 8.

- **Advertising aimed at children.** Issues surrounding advertising that is aimed at children and young people receive regular discussion and media coverage, most recently in relation to the debate on childhood obesity.[10] While some argue that, because of their vulnerabilities, it is an invasion of a child's right to privacy to be targeted by advertising, the ALRC does not consider that this is a privacy issue. However, the Inquiry will consider the collection of personal information that can be used for direct marketing aimed at children and young people.

- **Censorship to protect children from explicit material, particularly in the online environment.** This issue is hotly debated, with child protection on one side versus rights of free speech on the other.[11] This Inquiry will not consider censorship issues or issues relating to safety of children using the internet. It will, however, look at ways in which personal information of children and young people can be obtained and used for commercial purposes, particularly through the online environment.

Privacy rights of children and young people at international law

9.8 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).[12]

> 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.

---

8 See, eg, C Nader, 'Parents Out of the Loop on Baby Tests', *The Age* (online), 15 August 2006, <www.theage.com.au>.

9 The report recommends that that the Australian Health Ministers' Advisory Council, in cooperation with a number of other bodies, develop national standards in relation to the development and implementation of newborn screening programs: Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Rec 24–1. In its response to the report, the Australian Government supported this recommendation.

10 See, eg, J Robotham and J Lee, 'Fat Chance of Avoiding Hard Sell', *Sydney Morning Herald* (online), 27 July 2006, <www.smh.com.au>.

11 See, eg, J Stanley, *Child Abuse and the Internet: Child Abuse Prevention Issues Paper 15* (2001) National Child Protection Clearinghouse.

12 *Convention on the Rights of the Child*, 20 November 1989, [1991] ATS 4, (entered into force generally on 2 September 1990).

> 2. The child has the right to the protection of the law against such interference or attacks.

Article 40(2)(b)(vii) refers to the specific need to have respect for the privacy of a child accused or found guilty of a criminal offence.

9.9 The articles cover the concept of 'privacy' as 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 with others.[13] 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.[14]

9.10 CROC was adopted by the United Nations in November 1989 and ratified by Australia in December 1990, coming into effect for Australia in January 1991. It is the most universally accepted international convention.[15] Any federal, state or territory legislation, policy or practice that is inconsistent with CROC places Australia in breach of its international obligations.[16]

9.11 A number of other international guidelines relating to the rights of children make reference to the need to protect the privacy of children, including the *United Nations Standard Minimum Rules for the Administration of Juvenile Justice 1985* (the Beijing Rules)[17] and the *United Nations Rules for the Protection of Juveniles Deprived of Their Liberty 1990*.[18] Although not necessarily binding on Australia at international law, the guidelines represent internationally accepted minimum standards and are important reference points in developing policy.

---

13 Unicef, *Implementation Handbook for the Convention on the Rights of the Child* (fully revised ed, 2002), 213.

14 J Doek—Chairperson UN Committee on the Rights of the Child, *Consultation PM 14*, Sydney, 18 August 2006.

15 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].

16 Except in relation to art 37(c).

17 *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.

18 *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.

9.12 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 they believe to be most appropriate.[19] 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 or the rights recognized in the present Convention.

9.13 CROC is therefore 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.[20]

9.14 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 given a greater understanding of children's cognitive abilities and prompted a re-evaluation of rules regarding children's capacity.[21] Increasingly the common law and particular statutes are recognising the ability of young people above a certain age to make decisions on their own behalf, even where this may conflict with the wishes of their parents.[22]

---

19 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.

20 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).

21 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].

22 See in particular *Gillick v West Norfolk and Wisbech AHA* [1986] AC 112 and *Re Marion* (1992) 15 Fam LR 392.

9.15 Consistent with CROC, most rights and responsibilities in Australian law refer to a person as an adult when they turn 18 years of age.[23] In recognition of the transition phase between childhood and adulthood, this chapter adopts terminology making a distinction between a 'child' and a 'young person'. In the past the ALRC has linked a 'child' with a person under the age of 12, and a 'young person' as a person aged 12 to 17 (inclusively).[24] This age distinction is intended to facilitate discussion, and is not intended to pre-empt any policy decision on definitional issues that the ALRC might make in relation to children and young people as part of this Inquiry.

Existing Australian laws relating to privacy of children and young people

Privacy Act 1988 (Cth)

9.16 As for all adults, the personal information of children and young people is regulated by a number of laws. The laws that apply will depend upon who holds the information.[25]

- Personal information held by Commonwealth and ACT public sector agencies or their contactors is regulated by the Information Privacy Principles (IPPs) in the *Privacy Act*.

- Personal information held by non-government bodies is regulated by the National Privacy Principles (NPPs) in the *Privacy Act*, so long as the body is not exempt from the operation of the Act. Personal information which falls within the definition of 'sensitive information', including health information, is subject to a higher level of privacy protection.

- Personal information held by state or territory public sector agencies may be regulated by particular state or territory legislation.

9.17 Chapter 3 provides a full overview of the operation of the *Privacy Act*. The Act is stated to apply to natural individuals, and makes no reference to age. The Act contains no particular provisions relating to children or young people, but applies equally to adults and to children and young people.

9.18 Many aspects of the IPPs and the NPPs involve the concept of awareness or consent of an individual to collect, use or disclose their personal information. For

---

23 Although this varies, particularly in the area of juvenile justice: see L Blackman, *Representing Children and Young People: A Lawyers Practice Guide* (2002), 4–5.

24 Australian Law Reform Commission and Human Rights and Equal Opportunity Commission, *Seen and Heard: Priority for Children in the Legal Process*, ALRC 84 (1997).

25 For a more detailed analysis of the scope of existing privacy laws in Australia see Ch 2.

example, IPP 2 says that an agency that asks for personal information normally must tell the person why it is collecting the information and to whom it usually gives that sort of information. Where the information is provided voluntarily, it is assumed that, based on the information supplied by the collector, the individual will make a choice as to whether the information will be given. NPP 2.1 requires that personal information will not be disclosed for a purpose other than the primary purpose for which it was collected except in particular circumstances, one of which is that the individual consents to the use or disclosure. Both examples assume that the individual is capable of understanding the relevant issues and communicating their consent to the collection or disclosure of the information.

9.19 The Act sets no age limit on when 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.[26]

9.20 The *Guidelines on Privacy in the Public Health Sector* stress that, in circumstances 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.[27] 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.[28]

9.21 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 care or treatment of the individual for compassionate reasons. A 'responsible' person is defined to include a parent of the individual.[29] No other NPP and no IPP sets up a structure for making decisions on behalf of an individual unable to make a privacy decision.[30] It is assumed that parents

---

26 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.

27 Office of the Federal Privacy Commissioner, *Guidelines on Privacy in the Private Health Sector* (2001), 33.

28 Ibid, 34.

29 *Privacy Act 1988* (Cth) sch 3, NPP 2.5. 'Parent' is defined to include a step-parent, adoptive parent and foster-parent: *Privacy Act 1988* (Cth) sch 3, NPP 2.6.

30 See discussion of adults with a decision-making disability in this chapter.

will have responsibility for making decisions on behalf of children or young people incapable of making the decision themselves.[31]

Other privacy legislation

9.22 Some states and territories have legislation or administrative practices which regulate the privacy of certain personal information held by state or territory public sector agencies.[32] Most apply specifically to health information and these are discussed in more detail in Chapter 2.

9.23 Generally, these statutes and schemes adopt the same approach to children and young people as the federal *Privacy Act* in that children and young people are given the same rights and protections as adults. However, unlike the federal *Privacy Act*, 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, the *Health Records Act 2001* (Vic) states that a child will be deemed incapable of giving, making or exercising a consent, request or right if, despite reasonable assistance by another person, he or she is incapable by reason, first, of understanding the general nature and effect of giving, making or exercising such consent, request or right, or, secondly, of communicating such consent or refusal of it, making such a request or personally exercising such a right.[33] In the *Health Records (Privacy and Access) Act 1997* (ACT), the test of capability is linked to the ability to understand the nature of, and give consent to, a health service.[34] 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 decision.

9.24 There is no privacy legislation in the states or territories that provides protections for personal information particular to children and young people.

---

31 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 213.

32 For an overview of privacy regulation in the states and territories, see Ch 2.

33 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. The *Health Records and Information Privacy Act 2002* (NSW) s 7 has a similar operation.

34 '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.

Areas pertinent to privacy of children and young people

Child welfare

9.25 The protection of children and young people from abuse and neglect is deemed more important in some situations than an individual's right to privacy.[35] All states and territories have laws in place which in practice provide exceptions to privacy laws by allowing or requiring disclosure of personal information in certain circumstances. Taking New South Wales as an example, these provisions include obligations to provide or exchange information with the Department of Community Services and the Children's Guardian regarding the safety, welfare and wellbeing of a child or young person;[36] disclosure of information to the Ombudsman when exercising child protection functions;[37] and mandatory obligations on certain professionals to report a suspicion that a child is at risk of harm.[38]

9.26 A particular 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. The New South Wales Child Death Review Team has noted that a failure to provide information to the Department of Community Services has been a contributing factor in a number of cases where a child was killed by his or her parent.[39] This is particularly apparent in cases where the parent has a mental illness, including fatalities occurring during an episode of parental depression, and others where the parent was experiencing acute psychotic symptoms. The Review Team identified that the 'primary deficiency in service provision for this group involved a failure to consider the safety implications for the child of the parent's behaviour'.[40] In some of these cases concerns regarding privacy laws or duties of confidentiality have been cited as reasons why the information was not reported to the relevant government agency.[41]

9.27 The New South Wales Department of Community Services is presently reviewing the *Children and Young Persons (Care and Protection) Act 1998* (NSW). 'Options to authorise the release of information to the public about children and young people in particular circumstances, especially in the context of privacy legislation' has been identified as a key issue of the review.[42] The Department is due to report by 5 December 2006.

---

35 New South Wales Government Department of Community Services, *New South Wales Interagency Guidelines for Child Protection Intervention* (2005), 53.

36 See, eg, *Children and Young Persons (Care and Protection) Act 1998* (NSW) ss 185, 248.

37 See, eg, *Ombudsman Act 1974* (NSW) pt 3A.

38 *Children and Young Persons (Care and Protection) Act 1998* (NSW) s 27.

39 Child Death Review Team, *Fatal Assault of Children and Young People: Fact Sheet* (2003) New South Wales Commission for Children and Young People.

40 Ibid, 5. See also Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

41 New South Wales Commission for Children and Young People, *Consultation PC 34*, Sydney, 18 July 2006.

42 New South Wales Government Department of Community Services, *Review of the Children and Young Perons (Care and Protection) Act 1998: Issues Paper* (2005).

9.28 A recent report prepared for the Western Australian Ministerial Advisory Council on Child Protection recommended that privacy legislation should include an exemption for the bona fide exchange of information for the protection of children, with the exemption extending to individuals and organisations as well as government agencies.[43]

9.29 The ALRC is interested to hear if the *Privacy Act* or privacy legislation of the states and territories is contributing to problems regarding the sharing of information in circumstances where the safety of a child or young person is at issue.

Juvenile justice

9.30 Children and young people who come into contact with the juvenile justice system often have large amounts of information collected about them. This information can be viewed as particularly sensitive given the strong focus in juvenile justice on rehabilitation and reintegration into society,[44] and of even higher sensitivity if no charges are laid, charges are dropped or a finding of guilt is not made. The particular sensitivity is also reflected in the existence of international guidelines dealing specifically with the administration of juvenile justice which include provisions relating to privacy of information about the juvenile.[45]

9.31 State and territory juvenile justice legislation generally provides for the protection of information relating to a child or young person dealt with under the legislation. Taking Queensland as an example, identifying information about the child, a range of reports made or obtained in administration of the Act, and records or transcripts of court proceedings are considered to be confidential information and as such are given special protection.[46] Disclosure is only permitted in prescribed circumstances, most of which relate to administration of the Act. Disclosure can be made for research purposes if the anonymity of the information is preserved.[47] There is a prohibition on the publication of identifying information about a child.[48]

---

43 R Cant and T Simpson, *Myths and Realities—Sharing Information between Agencies to Enhance the Safety of Children and Young People* (2005) Western Australian Government Ministerial Advisory Council on Child Protection, 23. As Western Australia does not at present have privacy legislation applying to state government agencies, the recommendation referred to 'future' privacy laws.

44 Although courts can vary greatly in the weight they give to these various principles: see J Bargen, 'Community-Based Programs' in A Borowski and I O'Connor (eds), *Juvenile Crime, Justice & Corrections* (1997) 372, 374.

45 *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985), r 8; *United Nations Rules for the Protection of Juveniles Deprived of Their Liberty*, UN Doc A/RES/45/113 (1990), r 19.

46 *Juvenile Justice Act 1992* (Qld) pt 9.

47 Ibid s 297.

48 Ibid s 301.

9.32 The ALRC is interested to hear if there are any concerns in the area of juvenile justice about the operation of the *Privacy Act* or privacy legislation of the states and territories.

Family law

9.33 Children and young people will often be involved in counselling or family dispute resolution services undertaken as part of a family law dispute. This is an area where professional obligations regarding confidentiality overlap with specific legislative provisions regarding privacy and disclosure in certain circumstances.[49]

9.34 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.[50] The *Family Law Act 1975* (Cth) includes provisions governing the confidentiality of such services.[51] In general, communications—which includes the giving of personal information—made during counselling or family dispute resolution should not be disclosed, but there are a series of circumstances in which disclosure may be required or authorised.[52] For example, disclosure is required if it is necessary to comply with the law, which will include in those states and territories where there are mandatory reporting requirements if there is a suggestion that a child has been abused or is at risk of abuse.[53] The exception which allows disclosure of information for research purposes specifically excludes the disclosure of personal information as defined in the *Privacy Act*.[54] While an adult can give permission to have their information disclosed for any purpose, information provided by a person under the age of 18 can only be disclosed with the agreement of both parents, or approval of the court.[55]

9.35 The ALRC is interested to hear if there are any concerns about the interaction of ethical duties and legislative provisions relating to confidentiality and the *Privacy Act* in the area of family law, particularly given that some individuals and bodies providing confidential services are not subject to the provisions of the *Privacy Act*.

---

49 See discussion on privacy, confidentiality and secrecy provisions in the medical context in Ch 8.

50 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.

51 *Family Law Act 1975* (Cth) ss 10D, 10H. These provisions became operational on 1 July 2006.

52 These include where it is believed to be necessary to protect a child from harm, to prevent or lessen a serious or imminent threat to the life or health of a person or to the property of a person, to report the commission of an offence involving violence or a threat of violence to a person or damage to the property of a person, or where a child's interests are represented by an independent lawyer and disclosure would assist the lawyer: Ibid ss 10D(4), 10H(4).

53 See, eg, *Children and Young Persons Act 1989* (Vic) s 64(1A), (1C).

54 *Family Law Act 1975* (Cth) ss 10D(5), 10H(5).

55 Ibid ss 10D(3), 10H(3).

Health information

9.36 As noted above, the ALRC will not be dealing with consent to medical treatment as part of this Inquiry. Consent to the handling of health information of 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,[56] 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, however, and the pivotal case in this area is the House of Lords decision of *Gillick v West Norfolk and Wisbech AHA* (*Gillick*),[57] which was followed by the High Court of Australia in the case of *Re Marion*.[58] 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.[59]

9.37 Neither *Gillick* nor *Re Marion* 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.[60]

9.38 The ability of young people to keep information from their parents and others is often an important component of their medical treatment. This issue is often discussed as 'confidentiality', but the application of the *Privacy Act* and relevant state and territory health information legislation will also regulate the disclosure of health information.[61]

9.39 Young people experience a number of barriers in accessing health services, such as embarrassment, cost, inconvenient location or hours of services, and inexperience

---

56 *Minors (Property and Contracts) Act 1970* (NSW) s 49(2) for persons aged 14 years and above; *Consent to Medical and Dental Procedures Act 1985* (SA) s 6(1) for persons aged 16 years and above. See also New South Wales Law Reform Commission, *Minors' Consent to Medical Treatment*, IP 24 (2004).

57 *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.

58 *Re Marion* (1992) 15 Fam LR 392. This case involved an application before the Family Court of Australia for the sterlisation 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.

59 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).

60 J Loughrey, 'Medical Information, Confidentiality and a Child's Right to Privacy' (2003) 23 *Legal Studies* 510, 512.

61 For a discussion of the relationship between confidentiality and privacy in the medical field see Ch 8.

recognising health needs or where to seek help.[62] With worrying trends of worsening mortality and morbidity amongst young people, there is a need to reduce barriers and support positive health and help-seeking behaviours.[63] Lack of confidentiality (or a perceived lack of confidentiality) is a key barrier that has been identified in relation to young people.[64] A United States 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.[65] These concerns regarding confidentiality can be exacerbated in small communities, particularly in rural areas, where it is difficult to remain anonymous.[66]

9.40 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.[67] 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.[68] In most cases involving sensitive or serious health concerns, it is suggested that parental involvement be encouraged, and in many cases involvement of supportive parents may be a key element of successful treatment.[69] However, it is not always possible or desirable to involve a parent or guardian in this way.

---

62 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, 101–102.

63 L Sanci, M Kang and B Ferguson, 'Improving Adolescents' Access to Primary Health Care' (2005) 183 *Medical Journal of Australia* 416, 416.

64 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.

65 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.

66 See, eg, study of access to sexual health services by young people in rural communities in the United Kingdom: R Garside and others, 'Anonymity and Confidentiality: Rural Teenagers' Concerns when Accessing Sexual Health Services' (2002) 28 *Journal of Family Planning and Reproductive Health Care* 23.

67 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.

68 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).

69 T Stutt and L Nicholls, *Submission PR 40,* 11 July 2006.

9.41 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 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.[70] There is, however, a debate about whether the ability to request non-disclosure is separate from the ability to make a decision regarding treatment. There will, of course, be situations in which the doctor is required to disclose information and even for adults there are ethical, statutory and common law exceptions to the duty of confidentiality which require disclosure of information in certain circumstances.[71] 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.[72] Thus, in terms of privacy regulation, the argument would be that, subject to appropriate exceptions, the health information of a young person should be not be able to be disclosed to parents without the young person's consent.

9.42 This issue of disclosure of health information to parents was the subject of public debate in 2003 and 2004. The debate was sparked in 2003 when the Health Insurance Commission[73] changed its privacy policy so that young people aged 14 and over are required to give consent before their parents can access their Medicare records.[74] The policy states that:[75]

---

70 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.

71 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.

72 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.

73 Now known as Medicare Australia.

74 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).

75 The policy is set out on the Medicare Australia form 'Request for Obtaining Medicare and/or PBS Claims History for a Child'.

- if a child or young person of any age has their 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;[76]

- for a young person aged 14 or 15 on their 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;

- disclosure of information relating to a young person aged 16 and over on their parent's Medicare card will only be made available to a parent or legal guardian with the young person's consent.[77]

9.43 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 condition.[78]

9.44 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.[79] 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.[80]

---

76 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.

77 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.

78 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.

79 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 their 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.

80 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>.

However, following staunch opposition from certain backbenchers, the AMA and others, introduction of the Bill was deferred.[81] It has not since been introduced.

9.45 The *Privacy Act* and other Australian health information laws reflect the approach taken in medical practice and do not prescribe age limits 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.[82] 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. 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.

9.46 The ALRC is interested to hear if there are concerns about the operation of the *Privacy Act* in relation to disclosure to parents of health information of children and young people. If there are particular concerns, the ALRC would like to hear about possible options for addressing them.

Schools

9.47 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 and 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 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.

9.48 Schools are viewed by some as an untapped resource of information about children and young people. It provides a ready access point for marketers and researchers.[83] As children and young people in a school environment are used to

---

81 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>.

82 The *Privacy Act 1993* (NZ), *Health Information Privacy Code 1994* (NZ) and *Data Protection Act 1998* (UK) also operate in this way.

83 See, eg, Consumer's Union Education Services Division, *Selling America's Kids: Commercial Pressures on Kids of the 90's* (1998); and N Willard, *Capturing the 'Eyeballs' and 'E-wallets' of Captive Kids in School: Dot.com Invades Dot.edu* (2000) Center for Advanced Technology in Oregon, which outlines the situation in the United States where dot.com companies offer free technology resources to schools supported by an online advertising program that involves the collection of market-related personal information from students and targeted marketing of students with banner ads.

'obeying' instructions to participate in school projects, collaborations between schools and researchers can be particularly effective sources for researchers, whether for commercial or non-commercial purposes. This Inquiry will not consider the ethics of permitting researchers to enter schools and access children and young people within the school environment. However, the Inquiry is interested in considering how schools may collect, store and disclose personal information about children and young people.

9.49 With the exception of the ACT, government schools are not covered by the *Privacy Act* but will be subject to any state or territory privacy legislation or scheme covering the public sector.[84] Some states and territories have a privacy policy or privacy code which applies to all of its schools.[85]

9.50 Private schools are covered by the *Privacy Act* so long as they do not fall within the small business exemption. 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 nurses and other health professionals) is regarded as 'health information' and is regulated by the Act.[86] The OPC takes the view that in most instances private schools and colleges are covered by the Act and should comply with the NPPs.[87]

9.51 One of the key issues relating to access to records of a child or young person will be whether the school can disclose a record to a parent of the child or young person. In the private school context, it will generally be the parents who are entering a contract with the school to provide a service. However, schools subject to the NPPs must only disclose personal information regarding the child or young person consistently with the NPPs.

9.52 Advice from the OPC suggests that most information collected by a private school could be disclosed to parents as, under NPP 2.1(a) regarding a related second purpose, in most cases students would reasonably expect disclosure to parents. The OPC indicates that this will include school reports and also non-education related material such as health information or counselling records.[88] For older students, however, these expectations may differ in relation to some sensitive records. Research suggests that a key reason why young people do not use school counsellors is because

---

84 See Ch 2 for an overview of state and territory privacy laws.

85 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.

86 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 2006.

87 Ibid.

88 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 2006; 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 2006.

of concerns regarding confidentiality.[89] The OPC suggests that it is good practice, particularly for older students, for schools to have a policy on disclosure of records that is made available to parents and students.[90] 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.[91] However, it appears that at least some schools have adopted an alternative approach to at least some records of older young people.[92] Further, many schools have developed policies or practices specifically dealing with the publication on their websites of photographs or videos depicting children and young people.[93]

9.53 The ALRC is interested to hear about the way in which public and private schools collect, store and disclose personal information, and whether any concerns arise from these practices.

Child care services

9.54 A growing number of Australian children come into contact with formal child care prior to commencing school.[94] As with schools, child care services collect a vast amount of personal information about a child, and his or her family, in order to properly provide a service. This will include personal contact details of the child and any carers, health and dietary requirements, court orders, photographs and video, and records on the development of the child. In some child care centres, security arrangements have been put into place which require additional information to be added to a record. For example, at one centre that has introduced biometric identification, index fingerprints and digital photographs of any person who will drop off or pick up a child from the centre must be kept on file.[95]

---

89 W Reid, *School Counselling: A Client Centred Perspective* (1996) Kids Help Line, 10.

90 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 2006.

91 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* (1990)..

92 Private Individual, *Submission 73 to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, 2004.

93 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 2006 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.

94 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).

95 L Timson, 'Security and Peace of Mind for All Ages', *Sydney Morning Herald* (online), 1 August 2006, <www.smh.com.au>.

9.55 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.

9.56 The application of privacy laws to the child care sector is confusing.[96] Larger private or non-profit businesses running child care centres will be subject to the NPPs in the *Privacy Act*, but many smaller centres, most non-profit services and individuals running a service within their own home will be exempt as a small business from the operation of the *Privacy Act*. However, some otherwise exempt small businesses may fall within the definition of a health service provider under the *Privacy Act* or state health information legislation.[97] Any services operated by a state, territory or local council will be subject to any existing state or territory privacy legislation or scheme.

9.57 National standards have been developed for child care services, and have been utilised to inform child care regulations, funding guidelines and information resources.[98] 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) which is required to be kept confidential, although they differ on advice as to when that information may be disclosed.[99] The standards are not as comprehensive as any existing privacy principles. Some child care centres have their own privacy policies in place to govern the collection, use and disclosure of personal information.

---

96 Until 2000 child care service providers which 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.

97 For an example of 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 27 June 2006.

98 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.

99 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.

9.58 In the May 2006 Budget, it was announced that a National Child Care Management System would be phased in to make the industry more accountable.[100] While details have not yet been released, initial options that have been discussed include requiring parents to 'swipe' a card or enter a PIN number upon dropping off and picking up a child.[101] There is also a suggestion that, if introduced, a card will be linked with the proposed Access Card.[102] This information will be linked to the Centrelink-administered Child Care Benefit scheme. Non-compliance with the new system will mean that parents using that child care service will not be eligible to claim the Child Care Benefit. While most centres already use administration software to report attendances for benefit payments, and from 1 July 2006 all services are required to advise of vacancies by phone on a weekly basis, there are issues surrounding how much personal information may be required to be disclosed as part of this new system, and what controls should be in place to protect that information.[103]

9.59 The ALRC is interested to hear about the way in which child care services collect, store and disclose personal information, and whether any concerns arise from these practices.

Online consumers

9.60 Personal information collected in the online environment is subject to the same laws as any other personal information. This chapter will focus on personal information collected in the online environment explicitly, such as through registration pages, survey forms, order forms, and online contests. Chapter 11 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.

---

100 M Brough (Minister for Families Community Services and Indigenous Affairs), '2006–07 Budget—A More Responsive, Quality Child Care System' (Press Release, 9 May 2006).

101 S Peatling, 'Child ID Cards in Swipe at Fraud', *Sydney Morning Herald* (online), 2 June 2006, <www.smh.com.au>.

102 L Timson, 'Security and Peace of Mind for All Ages', *Sydney Morning Herald* (online), 1 August 2006, <www.smh.com.au>. For discussion on the Access Card proposal, see Ch 12.

103 Personal information collected from child care services by the Australian Government Department of Family, Community Services and Indigenous Affairs is subject to the IPPs in the *Privacy Act* and, where appropriate, the confidentiality provisions contained in *A New Tax System (Family Assistance) (Administration) Act 1999* (Cth). 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.

Children and young people as online consumers

9.61 The internet is an integral part of modern marketing techniques. Given their familiarity and high usage of the internet, and their significant consumer power,[104] it is not surprising that children and young people are targeted using this medium.

> 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.[105]

9.62 There is extensive literature which addresses the particular susceptibilities of children as consumers.[106] When combined with a medium that is often used by children and young people with little or no supervision, there are concerns about the privacy of children and young people as consumers using the internet.[107]

Online privacy regulation in Australia

9.63 The *Privacy Act* does not distinguish between the application of privacy principles in the online environment in contrast to any other field of activity. This means that 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. However, there is some criticism 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'

---

104 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].

105 Australian Direct Marketing Association, *Children and the Internet* (2005) <www.adma.com.au> at 21 June 2006.

106 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 24 July 2006; 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).

107 Issues surrounding the stalking of children on the internet are not covered by this Inquiry, although some of the techniques suggested for obscuring personal identity may be beneficial in protecting children from this kind of activity.

> including to disclose information to unspecified 'partners'; the small business exemption; and/or technological developments.[108]

9.64 A 2000 survey of the privacy practices of Australia's most popular 100 websites found that:

- although 72% of the sites surveyed collected personal information only 51% had a published privacy policy and only 28% of those sites notified users about the specific personal information that was collected;
- 71% of web sites with a stated privacy policy say that personal identifying information may be disclosed to third parties but one in three of those sites do not provide users with a choice about that disclosure;
- only 14% of the sites surveyed stated that users have the opportunity to have at least some personal information about them deleted from website records.[109]

9.65 The ALRC is not aware of any similar survey having been done since commencement of the *Privacy Amendment (Private Sector) 2000 Act* (Cth) and the NPPs. However, privacy has become smart business, whether or not an organisation is subject to the *Privacy Act*.

> From a purely commercial perspective, the need for good privacy practice is perhaps nowhere more pressing than in the online environment. Numerous surveys and reports in both Australia and the U.S. indicate that privacy concerns are a major factor restricting the development of e-commerce. Many consumers are unwilling to disclose personal information over the internet as a result of their lack of confidence in online privacy regarding how their information will be used by website operators. Reassuring consumers that their privacy will be respected is an essential step in encouraging consumers to transact online.[110]

9.66 The following initiatives relating to online privacy, and particularly online privacy of children and young people, have been developed in Australia in the absence of specific legislation:

- The OPC has issued *Guidelines for Federal and ACT Government World Wide Websites* which encourage best privacy practice for websites in compliance with

---

108 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.

109 Arthur Andersen and Andersen Legal, *Internet Privacy Survey 2000: A Survey of the Privacy Practices of Australia's Most Popular Web Sites* (2000), 1. This survey was based on the methodology of an internet privacy survey undertaken by the United States Federal Trade Commission in early 2000.

110 J Douglas-Stewart, *Comprehensive Guide to Privacy Law—Private Sector* (online), [40-6060] (22 August 2006).

the IPPs of the *Privacy Act*.[111] Guideline 1 recommends that a privacy policy be prominently displayed on the website. The policy should state: what information is collected; for what purpose and how this information is used; if it is disclosed, who is it disclosed to; and any other relevant privacy issues.

- The Australian Direct Marketing Association publishes tips on helping parents to safeguard a child's privacy online, and has plans to introduce guidelines on children's privacy that will be compulsory for its members.[112]

- Individuals 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, and using temporary email accounts.[113]

- The Internet Industry Association (IIA) has developed a Privacy Code of Practice which is currently under consideration by the OPC.[114] The Code includes a specific provision requiring that a legal guardian provide consent on behalf of a child under the age of 13 prior to disclosure of sensitive information collected from or about the child.[115]

Online privacy regulation in the United States

9.67 In contrast to Australia, the United States (US) has introduced federal legislation dealing with online privacy. The US Federal Trade Commission (FTC) has reviewed on a number of occasions privacy concerns relating to the operation of the internet industry. In 1998 and 1999, it determined that there was no present need for legislation to protect the online privacy of adult consumers; instead recommending the status quo of self-regulation.[116] In a further report in 2000, the FTC concluded that

> while self-regulatory efforts have achieved some real progress, the lack of broad-based implementation of such consumer protections online requires legislative action

---

111 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).

112 Australian Direct Marketing Association, *Children and the Internet* (2005) <www.adma.com.au> at 21 June 2006.

113 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* (2004), 64, 66.

114 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>.

115 Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001), [6.7]. The term 'child' is defined in [5.1].

116 United States Government Federal Trade Commission, *Self-Regulation and Privacy Online: A Report to Congress* (1999), 4, 12.

> in order to fully protect consumers' personal information and build public confidence in electronic commerce.[117]

9.68 In 2001, under the lead of a new Commissioner, the FTC indicated that new laws would impose substantial burdens on business, and instead increased resources for enforcement of existing privacy laws.[118] To date, no general online privacy legislation has been enacted at the federal level in the US.

9.69 A recent Canadian study looked at the online privacy operations of the top 100 business websites in the US and compared them with top business sites in the United Kingdom (UK), where online privacy is regulated and monitored by a government agency.[119] The researchers found that most web operators in both the US and the UK were 'open and honest' and protected user information appropriately, with only a small percentage of operators in both countries performing badly. However, the 'worst of the worst' were located in the regulated environment of the UK, and the UK operators were generally not as forthcoming as their US counterparts in disclosing how their sites operated and the purpose for which the information was gathered.

> You could tell the guys who were operating in the regulated market only disclosed what they were told they had to by law. Even then, what they wrote was mostly unreadable legalese …[120]

9.70 The US does have online privacy legislation dealing specifically with children. Based on the recommendations of the FTC,[121] the *Children's Online Privacy Act* (COPPA) was passed by the US Congress in 1998 with a requirement that the FTC issue and enforce rules concerning children's online privacy. 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 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. Foreign run websites must comply with COPPA if they are directed to children in the US. Under the Rule, operators are required to:

- post a clear and comprehensive privacy policy on their websites;

---

117 United States Government Federal Trade Commission, 'FTC Recommends Congressional Action to Protect Consumer Privacy Online' (Press Release, 22 May 2000).

118 Online Privacy Alliance, 'Online Privacy Alliance Applauds FTC's Plan to Devote More Resources to Enforcing Existing Privacy Laws' (Press Release, 10 April 2001).

119 University of Alberta, 'More Regulations Make Web Sites Less Trustworthy, Study Shows' (Press Release, 2 August 2006).

120 Ibid.

121 United States Government Federal Trade Commission, *Privacy Online: A Report to Congress* (1998).

- provide notice to parents and, with limited exceptions, obtain verifiable parental consent before collecting personal information;
- give parents the choice to consent to the collection and use of personal information of their child;
- provide parents 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.

9.71 The FTC 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.[122]

9.72 Website operators who violate the COPPA Rule could be liable for civil penalties of up to $11,000 per violation. The FTC undertook an active enforcement approach to COPPA, including 11 successful enforcement cases between 2000 and 2004,[123] and a published survey of the compliance levels of 144 key US websites.[124] 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.[125]

---

122 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 PIN or passwords.

123 All of these cases were settled. For details see the FTC website at <www.ftc.gov/privacy/privacyinitiatives/children_enf.html>. See also details of a more recent settlement against Xanga.com: D Caterinicchia, 'Xanga Settles with FTC for $1 Million', *Houston Chronicle* (online), 7 September 2006, <www.chron.com>.

124 United States Government Federal Trade Commission, *Protecting Children's Privacy Under COPPA: A Survey on Compliance* (2002). 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 from conditioning a child's participation in an online activity on the child's 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.

125 United States Government Federal Trade Commission, 'FTC Retains Children's Online Privacy Protection (COPPA) Rule Without Changes' (Press Release, 8 March 2006).

9.73 There have, however, been criticisms of the COPPA Rule and how it has operated in practice. These include:

- the fact that non-profit organisations are not covered by COPPA;[126]
- 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;[127]
- it is easy for children to circumvent the law by lying about their age, or open email accounts in their parents' names and give consent on their own behalf;[128]
- the substantial burden of complying with COPPA has forced many websites to simply eliminate children's programming;[129]
- 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.[130]

9.74 The ALRC is interested in hearing whether there is a need for more explicit regulation of personal information in the online environment in Australia, either generally or specifically in relation to children and young people.[131]

Photographs

9.75 As discussed above, this Inquiry is focused on privacy of personal information. 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.[132] 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*.

---

126 K Howard and Y Lim, 'Protection of Children in the Virtual World' (2005) 2 *Privacy Law Bulletin* 17, 19.

127 Ibid, 19.

128 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.

129 K Walker, 'The Costs of Privacy' (2001) 25 *Harvard Journal of Law & Public Policy* 87, 125.

130 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.

131 For more general discussion and questions relating to privacy and technology, see Ch 11.

132 *Privacy Act 1988* (Cth) s 6. For more detailed discussion of the definitions of 'record' and 'personal information', see Ch 3.

9.76 The photographing of children and young people has raised significant concerns in the past few years. Examples of situations in which photographs are being taken, and more particularly the way in which they are being disclosed on the internet, 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 regulating this issue.[133] The options included possible criminal offences regarding unauthorised use of photographs of children or voyeurism where an expectation of privacy exists, changes to the classification of online content, possible civil rights regarding unauthorised publication of images of people,[134] and education campaigns. The issue continues to be discussed in SCAG, with some jurisdictions pushing for uniform laws.[135]

9.77 The SCAG discussion paper includes extensive discussion of the issue of giving consent to the taking of a photograph, and how the absence of consent may greatly affect whether the taking of a photograph is considered to be unauthorised, and whether the subsequent use is connected with any consent that was given at the time the photograph was taken.[136] However, the SCAG discussion paper does not cover the issue of who should be able to provide consent where the person depicted is a child or young person. While it is assumed that parental consent is most appropriate for children, at what age would it be appropriate for a young person to be able to consent on their own behalf. What if the young person and the parent disagree? This issue will need to be considered if any of the options adopted by SCAG involve the concept of consent.

9.78 Many of the options raised in the SCAG discussion paper do not fall within the scope of the ALRC's current Inquiry. However, there may be options more closely related to the protection of personal information that could be pursued in conjunction with options taken up by SCAG. The ALRC will keep a watching brief on the outcomes of SCAG deliberations and will ascertain if there are further issues surrounding photographs that need to be considered more carefully as part of this Inquiry.

---

133 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].

134 While not referred to in the SCAG discussion paper, the ALRC has raised this in a previous report with a recommendation for a right of civil action in the case of publication of sensitive private facts relating to an individual without reasonable justification in circumstances where the publication is likely to cause distress, annoyance or embarrassment on an objective view of the position of the individual. Sensitive private facts were defined as matters relating to the health, private behaviour, home life, or personal or family relationships of an individual. This was specifically intended to include the publication of photographs taken in a private place without consent: Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (1979), [236]–[238]. The recommendation has not been implemented.

135 K Ngyuen, 'Law Chiefs have their Eyes on Voyeurs', *The Age* (online), 28 July 2006, <www.theage.com.au>.

136 See, eg, Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005), [31]–[38].

Broadcasting

9.79 Filming and broadcasting of children and young people may also raise issues of concern. Broadcasts may include images of children and young people, which fall within the definition of 'record' in the *Privacy Act*, or may include personal information otherwise identifying a child or young person.

9.80 A number of cases in New Zealand in 1999 heightened awareness regarding privacy issues and the filming and broadcasting of children. One involved a television broadcast involving an eight year old boy with Attention Deficit Disorder (ADD) and the problems his mother faced trying to look after him. Throughout the broadcast, the boy made it clear that he did not want to be filmed. In another case, a television broadcast showed a six year old boy, together with his parents, finding out who his father was after a paternity test.[137] Both of these cases involved filming and broadcasting of a child with parental permission.

9.81 In Australia, the 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 organisation.[138] 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 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'.[139]

9.82 The only set of Australian broadcasting standards or principles which deal specifically with the privacy of children is the *Commercial Television Industry Code of Practice*.[140] 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

---

137 For further details on these cases, 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 and K Ridley, 'Children and the Broadcasting Media: Respect for the Integrity and Rights of the Child?' (2000) 15(May) *Social Work Now* 6.

138 *Privacy Act 1988* (Cth) s 7B(4). For further discussion of the 'media exemption' see Ch 5.

139 Australian Communications and Media Authority, *Privacy Guidelines for Broadcasters* (2005), 1.

140 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.

> 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.

Section 4.3.5.2 states that 'child' means a person under 16 years.

9.83 While there has been a limited attempt by the commercial television industry in Australia to address issues of consent prior to naming or visually identifying a child or young person, the issue of whether parental consent is always appropriate has not been addressed. The New Zealand cases outlined above led to the Broadcasting Standards Authority of New Zealand amending the Privacy Principles that are imposed on broadcasters in that country to include an additional privacy principle relating especially to children.[141] A reworded principle similar to that inserted in 1999 still exists in the 2006 version of the Principles, with an additional principle which 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.[142]

9.84 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 for them are under stress.[143] This approach has not been incorporated into any particular guidelines issued within the industry.

9.85 Balancing the need to allow children to be involved in the media with ensuring the appropriate protection of their privacy can be a vexed issue. Requiring broadcasters to consider the best interests of a child, rather than relying on parental consent, places a significant burden on journalists and broadcasters. The ALRC is interested to hear whether there are particular concerns regarding broadcasting of images or other personal information of children or young people, and, if so, whether the *Privacy Act* is the appropriate place for providing solutions to these concerns.

Identification in court records

9.86 Information held by courts, including case files, judgments, and case management systems, will often identify children and young people who are somehow

---

141 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.

142 New Zealand Government Broadcasting Standards Authority, *Privacy Principles* (2006).

143 S Castell-McGregor, 'Children's Rights and the Media' (1985) 37 *Media Information Australia* 52, 53.

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.

9.87 The judicial records of courts are presently exempt from the *Privacy Act*.[144] Courts have traditionally been responsible for governing access to these records, and policies vary from court to court. However, as noted in Chapter 11, the advent of online access to court records opens up the ability for these records to be 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. Chapter 11 asks a question regarding the electronic publication of court records.

9.88 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.[145] Rule 8.1 of the Beijing Rules refers specifically to a young person's right to privacy at all stages of juvenile justice proceedings '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).[146]

9.89 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.[147] Stigma may attach to other cases such as immigration cases involving refusal of visas or applications for government payments.[148]

---

144 See discussion in Ch 5.

145 J Moriarty, 'Children, Privacy and the Press' (1997) 9 *Child and Family Law Quarterly* 217, 219.

146 *United Nations Standard Minimum Rules for the Administration of Juvenile Justice (the Beijing Rules)*, UN Doc A/RES/40/33 (1985), r 8 commentary.

147 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.

148 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 provides for non-publication of names of applicants for protection visas in the High Court of Australia, Federal Court of Australia or Federal Magistrates Court.

9.90 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.[149] Many Australian courts and tribunals have specific powers to make suppression orders under their establishing legislation.[150]

9.91 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.[151] 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.[152] The extent of the prohibitions vary, and in most cases the legislation permits, or a judge may permit, publication in certain circumstances.[153]

9.92 Many of the policy reasons behind these common law and legislative protections regarding identification of children or young people involved in proceedings are also relevant to discussions of providing access to court records. The ALRC is interested in hearing if there are particular issues relating to children and young people that should be considered as part of broader considerations of access to court records, particularly in the electronic environment.

Questions relating to children and young people

9.93 An examination of the areas outlined indicates that there are a number of recurring issues which arise when discussing privacy of children and young people.

9.94 One of the issues that arises is the existence of impediments to sharing of personal information in appropriate circumstances. While it has been highlighted in this chapter in relation to child welfare, the issue is not specific to children and young people. A more general discussion of the problems of inconsistent and fragmented

149 *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.

150 See, eg, *Federal Court of Australia Act 1976* (Cth) s 50; *Administrative Appeals Tribunal Act 1975* (Cth) s 35(2).

151 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.

152 *Family Law Act 1975* (Cth) s 121.

153 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.

privacy regulation and the need for mechanisms for appropriate sharing of personal information can be found in Chapter 7.

9.95 Most of the issues raised in this chapter are related to determining who should be able to make a decision or exercise a right regarding the personal information of a child or young person. At present, the *Privacy Act* has been interpreted as having a flexible system which allows for a case-by-case analysis to be made. Each individual child or young person is assessed to ensure that they have the capacity to make decisions and exercise rights on his or her own behalf. This is consistent with the recognition that children have evolving capacities. However, successful operation of an assessment model requires the collector of personal information to have some education or expertise in making such assessments, and can only be applied in circumstances where the collector has an opportunity to interact with the individual before making the assessment.

9.96 It is not always possible for transactions involving personal information to include an opportunity to assess the decision-making capacity of the individual. For example, when collecting personal information from an individual over the internet it is difficult to know how old the person is let alone to assess the decision-making capacity of that person. In such situations, collectors of personal information may be assisted by clear cut-off ages at which it is assumed that a person is able to make a decision on his or her own behalf.[154] In a cut-off model the collector can focus on developing a system for establishing the age of the individual, rather than an assessment of his or her decision-making capacity. The appropriate cut-off age may differ depending upon the sensitivity of the personal information and the use for which it is being collected.[155]

9.97 Regardless of which model is adopted for determining if a child or young person can lawfully make a decision or exercise a right regarding personal information, there is then a question of whether that automatically affects the ability of the parent or guardian to either: (a) make a decision or exercise a right in relation to the child or young person's personal information separately from the child or young person; (b) override a decision that has been made by the child or young person; or (c) access personal information which has been provided by, or collected about, the child or young person, without the consent of the child or young person, or against the express statement of the child or young person that the information not be disclosed to a parent or guardian. These are difficult questions, and the answers are likely to vary depending upon the situation, and the age and maturity of the child or young person.

---

154 There will always be situations where some people above the set age are not capable of making decisions: see the discussion on adults with a decision-making disability below.

155 As, for example, the sliding scale approach adopted in the COPPA Act discussed above.

9.98 A number of other issues arise regarding the personal information of children or young people.

- Many of the principles in the *Privacy Act* turn on the issue of express or implied consent. As discussed in Chapter 4, there are many concerns about providing informed consent in relation to privacy matters, and particular concerns when relying on implied consent. These concerns are multiplied when considering whether a child or young person has the relevant decision-making capacity to provide consent.

- There may be concerns about the accuracy of personal information collected from or about children and young people. This can stem from the inability (or perceived inability) of the child or young person to provide accurate information, and also from the rate at which the accuracy of personal information relating to a child or young person can change. This could have implications for privacy principles relating to accuracy of information and rights to have personal information updated or altered.

- Children and young people may be used as sources to collect personal information about people other than themselves. Chapter 4 contains a discussion on whether the privacy principles should include an obligation to collect information about an individual *only* from that individual.[156] The particular vulnerability of children and young people may need to be considered in deciding whether to apply any such principle.

- Chapter 4 also discusses openness principles. The application of such principles needs to be considered in the context of evolving capacities of children and young people who may be providing personal information, and whether a higher level of obligation is needed where collectors of personal information are particularly targeting children and young people.

9.99 The ALRC must consider these issues and whether they can, or should, be answered through amendments to the *Privacy Act*, other legislation or some other mechanism.

9.100 The ALRC would like to hear about other issues or situations relating to the personal information of children and young people which should be considered as part of this Inquiry.

156 At present the NPPs include this obligation, but the IPPs do not. See Ch 4.

Question 9–1 Should the protection of personal information for children and young people be dealt with expressly in the *Privacy Act*? If so, how should the Act be amended? For example, are there privacy issues arising in the areas of:

- child welfare, juvenile justice or family law;
- disclosure of health information to parents;
- information held by schools and child care centres;
- online consumer information;
- taking and publishing photographs;
- broadcasting of identifying images and information; or
- identification of children and young people in court records.

Question 9–2 Are there any other issues relating to the privacy protection of children and young people that are currently outside the scope of the *Privacy Act* that need to be addressed?

Adults with a decision-making disability

Equality

9.101 Unlike with children and young people, it is assumed that a person aged 18 or over has the capacity to make decisions on his or her own behalf. There are a range of reasons why an adult's capacity to make decisions may be impaired, including a mental illness, intellectual disability, dementia, brain injury or stroke.[157] The impairment could be permanent or temporary.

9.102 Although an adult with a decision-making disability may not be able to understand or 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

157 Privacy NSW, *Best Practice Guide: Privacy and People with Decision-Making Disabilities* (2004), 1.

> 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 …[158]

9.103 The United Nations has recently completed a draft international convention on the rights of persons with disabilities.[159] It is expected that the convention will be presented to the General Assembly for adoption at its next session, which commences in September 2006, and will then be open for signing and ratification.[160] The convention does not create new rights, but expresses existing rights in a manner that addresses the needs and situation of persons with disabilities.[161]

9.104 Article 22 of the draft 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.

9.105 The Australian Government participated in all negotiating sessions of the convention's working group.[162] If ratified by Australia, all legislation, policies and practices will need to be consistent with the new convention.

Problems with the *Privacy Act*

9.106 The need to ensure that privacy legislation enables people to act on behalf of others who cannot act for themselves has been raised in a submission to this Inquiry.[163] 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 live with a decision-making disability. While finding that the legislation generally worked well, in its submission to the OPC Review the AGAC indicated there was 'significant room for improvement in how a range of service providers interpret and

---

158 Ibid, 2.

159 The draft Convention on the Rights of Persons with Disabilities and Draft Optional Protocol is Annex II of: United Nations Ad Hoc Committee on a Comprehensive and Integral International Convention on the Protection and Promotion of the Rights and Dignity of Persons with Disabilities, *Draft Report on its Eighth Session*, A/AC.265/2006/L.6 (2006).

160 Human Rights and Equal Opportunity Commission, 'Disability to Make UN Top Ten' (Press Release, 26 August 2006).

161 United Nations, *International Convention on the Rights of Persons with Disabilities: Why a Convention?* (2006) <www.un.org/disabilities/convention/about.shtml> at 5 September 2006.

162 Human Rights and Equal Opportunity Commission, 'Disability to Make UN Top Ten' (Press Release, 26 August 2006).

163 K Bottomley, *Submission PR 10,* 1 May 2006.

apply the legislation in cases involving people who have a decision-making disability and their family members and allies'.[164]

9.107 Most of the concerns raised by the AGAC related to inflexible interpretation and application of privacy legislation by frontline staff involved in providing services, with financial institutions, utlities and insurance companies given as examples of where problems had arisen. Similar concerns were raised in stakeholder forums conducted as part of the OPC Review.[165] The problems primarily arise because businesses, in an attempt to comply with the NPPs, require an express authorisation from individuals so that another person can transact business on their behalf.

9.108 This issue is 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 serves as a substituted or assisted decision-maker. The existence of informal arrangements is consistent with the philosophy underpinning Australian guardianship and administration legislation which seeks to maximise involvement in decision making by the individual and ensure that the least restrictive alternatives are applied. Formal guardianship or administration orders are made as a last resort where informal arrangements have broken down.[166] Even in situations where a Power of Attorney or a formal guardianship or administration order is in place, concerns have been raised that these orders are not readily respected.[167]

9.109 The NPPs recognise that there will be circumstances in which an alternative person may need to make a decision or exercise a right on behalf of an adult.[168] For example, while NPP 2 establishes a general rule that personal information must only be used or disclosed for the primary purpose for which it was collected, exceptions to the general rule enable organisations to make judgments about disclosing an individual's personal information to a third party in certain circumstances.[169] The exceptions include where 'authorised by law', which would cover a circumstance where a formal guardianship or administration order has been made, allowing the appointed guardian or administrator to provide consent to disclosure on behalf of the individual.[170] NPP 6, which gives individuals a general right of access to personal information, will similarly

---

164 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.

165 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 215.

166 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.

167 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.

168 The range of circumstances differs in the IPPs and NPPs: see Ch 4.

169 For a full discussion of the operation of NPP 2 and the exceptions see Ch 4.

170 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 214.

allow a guardian or administrator to exercise a right on behalf of an individual where a formal guardianship or administration order is in place.[171]

9.110 The IPPs include more limited circumstances in which an alternative person may need to make a decision or exercise a right on behalf of an adult, but include where 'authorised or required by law' which would cover formal guardianship or administration orders.[172]

9.111 More sophisticated provisions exist in relation to health information of persons with a decision-making disability. NPPs 2.4, 2.5 and 2.6 establish a scheme that facilitates, within certain limits, disclosures of health information to 'responsible' persons.[173] The draft *National Health Privacy Code* goes a step further with more detailed provisions allowing an 'authorised representative' to give consent to the collection, use or disclosure of health information on behalf of an individual who is incapable of giving consent. However, for adults the provisions are still focused on 'authorised' representatives as recognised by law or a legal instrument. The operation of the NPPs and the draft *National Health Privacy Code* in relation to consent are discussed in detail in Chapter 8.

9.112 It is doubtful whether the exceptions currently covered by the *Privacy Act* provide adequate discretion to agencies and organisations to deal with informal guardianship arrangements and the concerns that have been raised, particularly in relation to non-health information.

9.113 In the OPC Review it was recommended that the Australian Government consider amending NPP 2 to permit a disclosure of non-health information in a similar way to which disclosure of health information can be made under NPP 2.4. The disclosure would be permitted 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.[174] The OPC also recommended the creation of more guidance to assist the development of appropriate practices consistent with the law, such as the best practice documentation in relation to people with decision-making disabilities that has been developed by Privacy NSW.[175]

9.114 The ALRC is interested in views relating to making decisions and exercising rights on behalf of adults with a decision-making disability under the *Privacy Act*.

---

171 Ibid, 215.

172 See, eg, *Privacy Act 1988* (Cth) s 14, IPP 11.

173 'Responsible' person is defined in Ibid sch 3, NPP 2.5.

174 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.

175 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).

Information sharing

9.115 Another issue that arises for adults with a decision-making disability is the need to facilitate access to personal information for the provision of appropriate services by government or non-government agencies. Particularly in circumstances where there is no alternative decision maker such as a legal guardian or family member, there can be problems in obtaining the necessary consent to disclose information in order that a vulnerable adult receives the protection and services he or she needs. 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.[176] Chapter 7 contains a general discussion of the problems of inconsistent and fragmented privacy regulation and the need for mechanisms for appropriate sharing of personal information.

Question 9–3 Is there a need to amend the *Privacy Act* to facilitate better the protection of the personal information of adults with a decision-making disability? If so, what amendments are required? Are there any non-legislative options that should be adopted in relation to adults with a decision-making disability?

176 Community Services Ministers' Advisory Council, *Submission PR 47,* 28 July 2006.

10. Telecommunications Privacy

Contents

Introduction

10.1 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. Prior to 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] However, since the introduction of the private sector provisions of the *Privacy Act,* 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.

10.2 A number of recent inquiries have considered the interaction between the regimes governing the protection of personal information in the telecommunications

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*.

industry 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.

10.3 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]

10.4 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.

10.5 This chapter outlines the different schemes that regulate the handling of personal information in the telecommunications context and examines the way in which these schemes interact with the *Privacy Act*. It also discusses legislation that has been introduced to control particular activities that occur in the telecommunications context that impact on privacy, such as telemarketing. The privacy of internet users and users of wireless technologies is discussed more generally in Chapter 11.

Personal information in the telecommunications industry

Telecommunications Act 1997 (Cth)

10.6 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

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.

6 *Telecommunications Act 1997* (Cth) s 7. A carrier licence is granted under s 56 of the *Telecommunications Act 1997* (Cth).

unguided electromagnetic energy.[7] A 'carriage service provider' is a person who uses infrastructure owned by a carrier to carry these types of communications.[8]

10.7 Part 13 of the *Telecommunications Act* regulates the use and disclosure of information obtained by certain bodies during the supply of telecommunications services. It makes it an offence (punishable by up to two year's imprisonment) for certain participants in the telecommunications industry—namely, carriers, carriage service providers, telecommunications contractors, eligible number database operators 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;
- the carriage services supplied or intended to be supplied by a carrier or carriage service provider; or
- the affairs or personal particulars (including any unlisted telephone number or any address) of another person.[9]

10.8 The Act specifies a number of exceptions to these 'primary use/disclosure offences'.[10] For example, any of the regulated bodies may use or disclose protected information if the use or disclosure is required or authorised by law,[11] or is necessary for law enforcement or business purposes.[12] The Act also regulates the secondary use and disclosure of protected information.[13] 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.[14] A person who contravenes the secondary use and disclosure provisions is also guilty of an offence punishable by up to two year's imprisonment.[15]

10.9 Part 13 of the Act requires carriers, carriage service providers and number database operators to create records of certain disclosures of protected information.[16] These records must be provided to the Australian Communications and Media

7 *Telecommunications Act 1997* (Cth) ss 7, 42.
8 Ibid ss 7, 16, 87.
9 Ibid ss 276–278.
10 Ibid ss 279–294.
11 Ibid s 280(1)(b).
12 Ibid ss 282, 283, 291.
13 Ibid ss 296–303A.
14 Ibid s 297.
15 Ibid s 303.
16 Ibid s 306.

Authority (ACMA) at the end of each financial year.[17] The Privacy Commissioner monitors compliance with the record-keeping requirements under the Act.[18] In 2004–05, there were 885,466 disclosures—an increase of 26% from the previous financial year.[19]

10.10 Part 6 of the *Telecommunications Act* deals with the development of industry codes and standards for particular industry activities. Industry codes and standards developed under the Act can deal with privacy, including the protection of personal information.[20] However, an industry code or standard cannot derogate from the requirements of the *Privacy Act*, or a privacy code approved under the *Privacy Act.*[21]

10.11 The Privacy Commissioner must be consulted about industry codes and standards that deal with privacy issues.[22] In 2004–05, the Privacy Commissioner provided advice in respect of 17 codes being developed pursuant to the *Telecommunications Act*.[23] 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 National Privacy Principles (NPPs) or an approved privacy code,[24] 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.[25]

Integrated Public Number Database (IPND)

10.12 Currently, Telstra's carrier licence requires it to provide and maintain an 'integrated public number database' (IPND).[26] 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.[27]

10.13 Section 472(1) of the *Telecommunications Act* allows the Minister (currently the Minister for Communications, Information Technology and the Arts)[28] to determine that a person other than Telstra should provide and maintain an IPND. However, any

17 Ibid s 308.
18 Ibid s 309.
19 Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 186.
20 *Telecommunications Act 1997* (Cth) s 113(3)(f).
21 Ibid s 116A.
22 Ibid ss 117(1)(j), (k), 134.
23 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), [1.8.1].
24 *Telecommunications Act 1997* (Cth) ss 121, 122.
25 Ibid s 282(8).
26 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*.
27 Ibid, cl 10(4).
28 Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004, sch pt 3.

such determination has no effect while Telstra's carrier licence requires it to provide and maintain an IPND[29] and, to date, no such determination has been made.

10.14 The *Telecommunications Act* requires carriage service providers to provide Telstra with as much information as is reasonably required to provide and maintain the IPND.[30] 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'.[31] At 30 June 2005, 24 carriage service providers provided data to the IPND and the IPND contained approximately 43.6 million records.[32]

10.15 Telstra's carrier licence limits the purposes for which information in the IPND can be used and disclosed.[33] It can only be disclosed to a carriage service provider to enable the provider to: provide directory assistance, operator assistance or operator services; to produce a public number directory; to provide location dependent carriage services; or to assist emergency call services and enforcement agencies.[34] In 2004–05, in addition to emergency service organisations and law enforcement agencies, there were seven authorised data users. Two of these data users were authorised to access the IPND to provide location-dependent carriage services and five were authorised to access the IPND to publish public number directories.[35]

10.16 Telstra's carrier licence also provides that access to information in the IPND is subject to Part 13 of the Act.[36] 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: (i) provision of directory assistance services by or on behalf of a carriage service provider; (ii) publication or maintenance of a directory of public numbers; or (iii) matter or matters raised by a call to an emergency service number.

10.17 In August 2000, the former Australian Communications Authority (now ACMA) registered an industry code governing the input, use, disclosure and storage of data in the IPND (the IPND Code).[37] The code aims to ensure that IPND information is accurate and up-to-date by, for example, requiring carriage service providers to supply

---

29 *Telecommunications Act 1997* (Cth) s 472(5).
30 Ibid s 101, sch 2 pt 4.
31 Ibid s 280.
32 Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 184.
33 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, cl 10 (7).
34 Ibid, cl 10(1).
35 Australian Communications and Media Authority, *Telecommunications Performance Report 2004–05* (2005), 184.
36 *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997*, cl 10(9)(b).
37 Australian Communications Industry Forum, *Integrated Public Number Database (IPND) Data Provider, Data User and IPND Manager*, ACIF C555 (2002). Industry codes and standards are discussed further below.

the IPND Manager (Telstra) with updated information each business day.[38] It also aims to ensure the secure storage of IPND data by, for example, requiring the IPND Manager to take all reasonable steps to protect the information from misuse, loss and unauthorised access, modification and disclosure.[39] The IPND Code also prohibits the use or disclosure of information in the IPND for any purpose other than those set out in Telstra's licence condition.[40]

10.18 In November 2003, the Australian Communications Authority (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*.[41]

10.19 In March 2004, the ACA released a discussion paper on regulating the use of IPND data[42] and in May 2005 it released a draft industry standard on the use of IPND data.[43] If determined, the draft standard would apply to the 'public number data' section of the telecommunications industry.[44] It would regulate further the use of IPND data; ensure that customers are aware of the purposes of the collection of IPND data and the purposes for which the information may be disclosed; and enable customers to choose whether to include their data in a public number directory. During 2005–06, the regulation of the use and disclosure of information sourced from the IPND remained the subject of consideration by ACMA and the Australian Government.

Interaction between the *Privacy Act* and the *Telecommunications Act*

10.20 When the private sector provisions were introduced into the *Privacy Act,* a new division was inserted into the *Telecommunications Act* to clarify the relationship between the use and disclosure provisions in the two Acts. The *Telecommunications Act* now 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.*[45] This means that 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. During the OPC Review*,* Telstra submitted that the fact that an authorised use or disclosure under

38 Ibid, 9.4.
39 Ibid, 7.5.
40 Ibid, 12.6.
41 These included 'database enhancement', 'data cleansing', 'data verification', and 'list management': Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004), 11.
42 Ibid.
43 Australian Communications Authority, *Draft Telecommunications (Use of Integrated Public Number Database) Standard* (2005).
44 This would be determined pursuant to s 110 of the *Telecommunications Act 1997* (Cth).
45 Ibid s 303B.

Part 13 did not amount to a breach of the NPPs should be made clearer, either by legislative amendment or guidance issued by the OPC.[46]

10.21 As noted above, Part 13 of the *Telecommunications Act* allows the use or disclosure of information where it 'is required or authorised by or under law'.[47] During the OPC Review, Electronic Frontiers Australia (EFA) submitted this could be interpreted as allowing the use or disclosure of information if that use or disclosure was permitted under NPP 2. EFA submitted that legislative amendment was needed to clarify this aspect of the interaction between the *Telecommunications Act* and the *Privacy Act*.[48]

10.22 In its review of the private sector provisions of the *Privacy Act*, the OPC recommended that the Australian Government consider amending the *Privacy Act* and the *Telecommunications Act* to clarify what are authorised uses and disclosures under the Acts.[49] It also indicated it would discuss with the ACA the development of guidance to clarify the relationship between the *Privacy Act* and the *Telecommunications Act*.[50]

10.23 Another provision introduced to clarify the interaction between the two Acts 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.[51]

Adequate protection of personal information?

The handling of personal information by telecommunications providers

10.24 With the exception of NPP 2, the use and disclosure principle, the NPPs regulate the handling of personal information by telecommunications providers. Accordingly, 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 telecommunications 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,

---

46 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, 11.

47 *Telecommunications Act 1997* (Cth) s 280(1)(b).

48 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, [48]–[51].

49 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.

50 Ibid, Rec 10.

51 *Telecommunications Act 1997* (Cth) s 303C.

52 *Privacy Act 1988* (Cth), sch 3, NPP 1.1.

such as the types of organisations to which the provider usually discloses the information.[53]

10.25 The ALRC is interested in hearing whether the NPPs protect adequately personal information collected by telecommunications providers or whether additional protections are required. In this regard, the ALRC notes that 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,[54] and to ensure that subscribers to telecommunications services are given the opportunity to determine whether their personal data are included in a public directory.[55] 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.[56] It requires Member States to retain telecommunications data for not less than six months and not more than two years from the date of the communication.[57] It also requires Member States to store the data securely, and to destroy the data that have not been accessed and preserved at the end of the retention period.[58]

10.26 The use and disclosure of information or a document about 'the affairs or personal particulars ... of another person' is governed by the *Telecommunications Act.* The circumstances in which such information can be used or disclosed under this Act differ from the circumstances in which personal information can be used or disclosed under the *Privacy Act.* As noted above, Part 13 of the *Telecommunications Act* makes it an offence to use or disclose the affairs or personal particulars of another person[59] except in specific circumstances.[60] Accordingly, it is arguable that Part 13 provides a higher level of protection of personal information than the NPPs because it criminalises the use or disclosure of personal information except in certain circumstances, while NPP 2 allows the use and disclose of personal information for: (i) the purpose for which it was collected; and (ii) for other secondary purposes (such as direct marketing) in certain circumstances.

10.27 It has also been argued, however, that many of the exceptions to the offence provisions in Part 13 are unnecessarily broad[61] and do not provide a sufficient level of

---

53 See Ibid sch 3, NPPs 1.3, 1.5.

54 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.

55 Ibid, art 12.

56 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.

57 Ibid, art 5.

58 Ibid, art 7.

59 See, eg, *Telecommunications Act 1997* (Cth) ss 276(1)(a)(iv), 277(1)(a)(ii), 277(1)(a)(iii).

60 Ibid pt 13 div 3 subdiv A.

61 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].

protection of personal information in the telecommunications industry. For example, organisations can use or disclose personal information if the person to whom it relates 'is reasonably likely to have been aware or made aware' that the information is usually disclosed or used in the circumstances.[62] Accordingly, it is also arguable that Part 13 actually provides a lower level of protection than the NPPs, which require certain secondary uses or disclosures to be 'related to' the primary purpose of collection.

10.28 The ALRC is interested in views on the appropriate standard of protection for the use and disclosure of personal information in the telecommunications industry. In particular, the ALRC is interested in whether the use and disclosure provisions under Part 13 of the *Telecommunications Act* protect adequately the privacy of personal information in the telecommunications sector, and whether the differences in these provisions and the NPPs are necessary and appropriate.

Regulatory gaps

10.29 The *Privacy Act* does not generally apply to businesses with an annual turnover of $3 million or less.[63] However, telecommunications providers in this category are obliged to comply with Part 13 of the *Telecommunications Act*. Accordingly, the use and disclosure of information by these providers is regulated by this Act. However, these providers are not required to observe any standards when engaging in other information handling practices that are dealt with in the NPPs, such as the collection and storage of personal information.[64]

10.30 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.[65]

---

62 *Telecommunications Act 1997* (Cth) s 289(B).

63 *Privacy Act 1988* (Cth) ss 6C, 6D. However, a business with an annual turnover of $3 million or less is bound by the NPPs in certain circumstances, such as in circumstances where the business discloses personal information about another individual for a benefit, service or advantage: see *Privacy Act 1988* (Cth) s 6D(4).

64 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.

65 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].

10.31 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.[66] The Senate Committee recommended that the small business exemption be removed from the *Privacy Act.*[67]

10.32 In Chapter 5 the ALRC asks whether the small business exemption should remain, and in Chapter 11 the ALRC asks whether the *Privacy Act* should be extended to apply to any exempt agencies or organisations that use certain types of technology or collect certain types of personal information.

Other issues

10.33 Another issue is the use of personal information by producers of public number directories who do not source the information from the IPND. The ACA has noted that Telstra's directory arm, Sensis, has a database of information provided to it by other telecommunications providers that enables it to publish the White Pages.[68] This information is also used for information management purposes, such as the 'MacroMatch' service, which 'electronically compares a contact database with the White Pages® database, appends the phone number where there are matches and produces a detailed evaluation report'.[69] The MacroMatch service is used by 'market research companies, call centres, direct mail houses, banking and finance, utilities, credit providers, debt collectors, superannuation and insurance companies'.[70] The ALRC is 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.

Regulatory bodies

10.34 Several bodies are involved in the regulation of the telecommunications industry. ACMA is a statutory authority[71] 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 Telecommunications Industry Ombudsman (TIO) is an industry body that investigates and determines complaints by users of carriage services,[72] including

66 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.
67 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 12.
68 Australian Communications Authority, *Who's Got Your Number? Regulating the Use of Telecommunications Customer Information*, Discussion Paper (2004), 8.
69 Sensis, *MacroMatch* <www.about.sensis.com.au/products/wp_macromatch.php> at 8 August 2006.
70 Ibid.
71 *Australian Communications and Media Authority Act 2005* (Cth) s 8(1).
72 *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 128(4).

complaints about privacy.[73] The OPC deals with complaints of interference with privacy in the telecommunications industry.

10.35 Each of these regulatory bodies receive privacy-related complaints from consumers. The ACA noted that concern about privacy was a key theme in the complaints it received in 2004–05.[74] In this same period, the TIO received 2,718 complaints relating to privacy of consumers with a landline, mobile telephone or internet connection.[75] Between 21 December 2001 and 31 January 2005, the OPC received 223 complaints about privacy in the telecommunications sector (approximately 9% of all NPP complaints) and 1,725 enquires about privacy in the telecommunications sector (approximately 4% of all NPP enquiries).[76] Further, these regulatory bodies have different powers to resolve complaints made by consumers. For example, the TIO has the power to order service providers to provide complainants with compensation of up to $10,000,[77] while there is no statutory limit on the amount of compensation that the Privacy Commissioner can award to a complainant.[78]

10.36 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;[79] and waste agency resources.[80] Telstra suggested that industry complaints bodies be given responsibility for considering privacy-related complaints at first instance, to ensure the efficient and timely investigation of complaints and to enable the OPC to focus on broader privacy issues.[81] The OPC noted that it could liaise closely with other privacy regulators to 'ensure that privacy complaints are handled efficiently and to minimise confusion and costs for both individuals and organisations'.[82] The ALRC is interested in hearing whether the existence of overlapping regulators in the telecommunications industry raises any issues.

---

73 *Telecommunications Industry Ombudsman Constitution*, 20 May 2006, cl 4.1.

74 Australian Communications Authority, *Annual Report 2004–05* (2005), 41.

75 Telecommunications Industry Ombudsman, *Annual Report 2004–05* (2005), 39, 47, 54.

76 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 51.

77 *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].

78 The powers of the Privacy Commissioner to make determinations are discussed in Ch 6.

79 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.

80 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].

81 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].

82 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 159.

The interception of telecommunications

Background

10.37 Laws relating to the interception of telecommunications were initially concerned with preserving the integrity of telecommunication systems.[83] However, in 1960 legislation was introduced to protect the privacy of individuals by making it an offence to intercept communications passing over telecommunication systems (with certain exceptions).[84] In 1979, this and other legislation governing the interception of telecommunications was repealed and replaced with the *Telecommunications (Interception) Act 1979* (Cth).[85] Since this time, there have been a number of inquiries into telecommunications interception[86] and numerous changes to interception legislation.[87]

10.38 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, the ALRC is of the view that the circumstances in which communications can be intercepted is an issue that is outside the scope of this Inquiry. However, federal legislation governing the interception of telecommunications 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)

10.39 The *Telecommunications (Interception and Access) Act 1979* (Cth) 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'[88] without the knowledge of the sender or intended recipient of the communication.[89] However, 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.[90]

---

83 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [753].

84 *Telephonic Communications (Interception) Act 1960* (Cth).

85 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [754]–[755].

86 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).

87 The history of legislation governing the interception of telecommunications is discussed further in Ch 1.

88 *Telecommunications (Interception and Access) Act 1979* (Cth) ss 6, 7. A 'stored communication' is a communication that has passed over a telecommunications system, is held on equipment used and possessed by a telecommunications provider, and can only be accessed with the assistance of an employee of the provider: See *Telecommunications (Interception and Access) Act 1979* (Cth) s 5.

89 *Telecommunications (Interception and Access) Act 1979* (Cth) s 108.

90 See, eg, Ibid ss 7(2)(a), 180(2)(d).

10.40 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.[91] 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.[92] It is possible that this type of information could also constitute 'personal information' for the purposes of the *Privacy Act.* Accordingly, the use and disclosure of information falling within these categories is subject to a different standard of protection than personal information under the *Privacy Act.*

10.41 The Act also contains a requirement that records of intercepted or stored communications be destroyed in certain circumstances.[93] Section 79 of the 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. In 2005, a report on a review of regulation of access to communications conducted by Mr Anthony Blunn (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.[94] Section 150 of the Act contains a similar requirement to destroy information or a record obtained by intercepting a stored communication. However, this section, introduced in 2006, does not distinguish between a record and a copy of a record. The Privacy Commissioner has expressed concern that the Act makes it lawful for an agency to keep information until such time as the chief officer considers whether it should be destroyed.[95]

10.42 Under the Act, law enforcement agencies are obliged to keep records relating to interception and stored communication warrants,[96] and to provide the Minister (currently the Attorney-General)[97] with an annual report containing information about these warrants.[98] The Minister is required to compile information received from law enforcement agencies into a report that must be tabled in Parliament.[99] Civil remedies are also available for unlawful interception of communications.[100]

---

91 Ibid pt 2.6, pt 3.4 div 2.
92 Ibid ss 63AA, 71, 134, 140.
93 Ibid s 150.
94 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, [9.4].
95 K Curtis (Privacy Commissioner), *Submission to the Senate Legal and Constitutional Legislation Committee Inquiry into the Provisions of the Telecommunications (Interception) Amendment Bill 2006*, 1 March 2006.
96 *Telecommunications (Interception and Access) Act 1979* (Cth) pts 2.7, 3.5.
97 Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004 sch pt 2.
98 *Telecommunications (Interception and Access) Act 1979* (Cth) pt 2.8 div 1, pt 3.6 div 1.
99 Ibid pt 2.8 div 2, pt 3.6 div 2.
100 Ibid pts 2.10, 3.7.

10.43 The Blunn Report concluded that the distribution of provisions relating to access of telecommunications data for security and law enforcement purposes between the *Telecommunications Act* and the *Telecommunications (Interception) Act 1979* (as it was then known) was 'complicated, confusing and dysfunctional'.[101] It recommended that comprehensive legislation dealing with access to all telecommunications and telecommunications data for law enforcement and security purposes be introduced.[102]

Monitoring of telecommunications

10.44 As noted above, the *Telecommunications (Interception and Access) Act* prohibits the monitoring of telecommunications, or access to stored communications, without the knowledge of those participating in the communication. Accordingly, if a participant in a communication has actual knowledge that it is being monitored—that is, that it is being listened to, read or recorded—the monitoring will not be an 'interception' and thus will not be unlawful under the *Telecommunications (Interception and Access) Act.* Agencies and organisations may monitor communications between employees and members of the public for a number of reasons, such as to provide training to employees.

10.45 An agency or organisation monitoring the communication may, however, still be governed by the *Privacy Act*. Neither the IPPs nor the NPPs require an organisation to obtain the consent of a person before collecting personal information by monitoring a communication (unless, in certain circumstances, the information is collected by an organisation and is 'sensitive information').[103] The Information Privacy Principles (IPPs) and NPPs also govern the use, disclosure, and storage of personal information collected by an agency or organisation that monitors communications with the knowledge of participants. In addition, telecommunication providers that monitor communications are required to comply with Part 13 of the *Telecommunications Act*.

10.46 The ALRC is interested in hearing whether laws relating to the interception of telecommunications adequately protect the privacy of personal information.

Other telecommunications privacy issues

Background

10.47 Many small businesses that use telecommunications services to engage in privacy-invasive practices are exempt from compliance with the *Privacy Act*. 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.

---

101 A Blunn, *Report of the Review of the Regulation of Access to Communications* (2005) Australian Government Attorney-General's Department, 6.

102 Ibid, Rec i.

103 *Privacy Act 1988* (Cth) s 14, IPPs 1, 2, 3; sch 3, NPPs 1.1, 1.2, 10.1.

10.48 In addition, NPP 2.1 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 privacy-invasive practices such as telemarketing. 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 elect not to receive any further direct marketing communications.

10.49 For these reasons, the *Privacy Act* has been unable to regulate some practices that interfere with privacy in the telecommunications context. Accordingly, two pieces of federal legislation have been 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).

Spam Act 2003 (Cth)

10.50 In 2003, legislation was introduced to prohibit the widespread practice of sending unsolicited commercial electronic messages (commonly known as 'spam'). 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.[104] The *Spam Act 2003* (Cth) prohibits the sending of commercial electronic messages via email, short message service, 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*.[105]

10.51 Consent can be express and inferred, although it may not be inferred from the mere publication of an electronic address.[106] Consent can, however, 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.[107] Regulations may specify in more detail the circumstances in which consent may or may not be inferred.[108] 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.[109]

---

104 National Office for the Information Economy, *Spam Act 2003: A Practical Guide for Business* (2004), 2.
105 *Spam Act 2003* (Cth) s 16. Direct marketing is discussed further in Ch 4.
106 Ibid sch 2 cl 4.
107 Ibid sch 2 cl 4.
108 Ibid sch 2 cl 5. To date, no such regulations have been made.
109 Ibid sch 2 cl 6.

10.52 The *Spam Act* requires lawful commercial electronic messages to contain certain information, such as information about the identity and contact details of the sender, as well as a 'functional unsubscribe facility'.[110] It also contains rules prohibiting the supply and use of 'address-harvesting software'[111]—that is, software that is used to search the internet for electronic addresses to compile or 'harvest'.[112] Ordinary telephone calls and facsimile communications are not covered by the Act.[113] Nor are certain types of electronic messages, such as purely factual messages or messages sent by registered political parties or charities.[114] ACMA has a range of powers to enable it to enforce the provisions of the *Spam Act*.[115]

10.53 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*[116] and the *Internet Industry Code of Practice*.[117] 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.

10.54 In its review of the private sector provisions of the *Privacy Act*, the OPC indicated it would discuss with the ACA the development of guidance to clarify the relationship between the *Privacy Act* and the *Spam Act*.[118]

10.55 In 2006 the Department for Communications, Information Technology and the Arts (DCITA) concluded a review of the operation the *Spam Act*.[119] DCITA found that the Act was operating successfully and should remain unchanged. However, it recommended 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'.[120] DCITA also recommended that the Australian Government undertake further consultation to determine whether facsimile communications should be regulated by the *Spam Act.*

---

110 Ibid ss 17, 18.
111 Ibid pt 3.
112 Ibid s 4.
113 Ibid s 5(5); *Spam Regulations 2004* (Cth) cl 2.1.
114 *Spam Act 2003* (Cth), sch 1.
115 Ibid 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.
116 Australian eMarketing Code Development Committee, *Australian eMarketing Code of Practice* (2005).
117 Internet Industry Association, *Internet Industry Spam Code of Practice* (2006).
118 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.
119 Australian Government Department of Communications Information Technology and the Arts, *Report on the Spam Act 2003 Review* (2006).
120 Ibid, Rec 22.

Do Not Call Register Act 2006 (Cth)

10.56 Telemarketing is the marketing of goods and services to the consumer by telephone. The ALRC examined telemarketing (and other forms of direct marketing) in its 1983 report on privacy (ALRC 22).[121] It noted that telemarketing was a nascent marketing strategy and that the majority of complaints about it did not involve privacy issues.[122] It recommended that the Human Rights Commission develop guidelines about telemarketing practices.[123]

10.57 Since ALRC 22, however, there has been a substantial increase in telemarketing activities,[124] and these activities are of increasing concern to the Australian public. For example, research into community attitudes to privacy conducted in 2004 revealed that 61% of respondents felt 'angry and annoyed' or 'concerned' when they received marketing material.[125] In 2004–05, the TIO received 887 complaints about telemarketing by consumers in receipt of landline telephone services.[126] In 2006, three out of four respondents to a national phone-in conducted by the ALRC nominated unsolicited telemarketing calls as their main privacy concern.[127] In addition, the ALRC has received several submissions to this Inquiry from stakeholders concerned about telemarketing activities.[128]

10.58 In 2005, the OPC recommended that the Australian Government consider: (i) amending the *Privacy* Act to provide consumers with a right to 'opt-out' of receiving all forms of direct marketing at any time;[129] and (ii) establishing a 'Do Not Contact' register.[130] 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.[131]

---

121 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [88], [252]–[260], [501]–[527], [688]–[691], [1174]–[1182].
122 Ibid, [257].
123 Ibid, [1182].
124 Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth).
125 Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (2004), [6.4].
126 Telecommunications Industry Ombudsman, *Annual Report 2004–05* (2005), 28.
127 Australian Law Reform Commission, 'Telemarketing, Information Privacy Top Community Concerns' (Press Release, 5 June 2006).
128 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; M Rickard, *Submission PR 19,* 1 June 2006; F Pilcher, *Submission PR 17,* 1 June 2006.
129 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.
130 Ibid, Rec 25.
131 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 15.

10.59 The *Do Not Call Register Act 2006* (Cth) establishes a scheme that 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 on Australians, as well as concerns about the impact of telemarketing on an individual's privacy'.[132]

10.60 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*.[133] The Act prohibits the making of unsolicited telemarketing calls to a telephone number on the Do Not Call Register without consent.[134] Consent can be express or inferred, although it cannot be inferred from the publication of the telephone number.[135] Regulations may specify in more detail circumstances in which consent may or may not be inferred.[136] 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.[137]

10.61 Telemarketers can request information from ACMA about whether a particular telephone number is on the register.[138] Numbers are registered for a period of three years, after which they are removed from the register until another valid application for registration of the number is made.[139] However, certain telephone calls, such as calls made by government bodies, religious organisations, registered political parties or charities in certain circumstances, are excluded from the operation of the Act.[140] In addition, certain telephone numbers, such as numbers used exclusively for the sending or receiving of facsimile communications, cannot be included on the register.[141]

10.62 ACMA will have a range of powers to enable it to enforce the provisions of the *Do Not Call Register Act.*[142] In addition, ACMA is required to establish a national industry standard to regulate certain conduct of all telemarketers, including those exempt from the operation of the Act.[143] This standard must address issues such as the time periods in which telemarketing calls can be made and the circumstances in which

---

132 Explanatory Memorandum, Do Not Call Register Bill 2006 (Cth).
133 *Do Not Call Register Act 2006* (Cth) ss 13–15. Direct marketing is discussed further in Ch 4.
134 Ibid s 11.
135 Ibid sch 2 cl 4.
136 Ibid sch 2 cl 5. To date, no such regulations have been made.
137 Ibid sch 2 cl 3.
138 Ibid s 20.
139 Ibid s 17.
140 Ibid sch 1.
141 Ibid s 14.
142 *Do Not Call Register (Consequential Amendments) Act 2006* (Cth) sch 1 pt 2.
143 *Telecommunications Act 1997* (Cth) s 125A.

a telemarketing call must be terminated. The Do Not Call Register is expected to be operational in 2007.[144]

10.63 The ALRC has been informed that the different definitions of consent under the *Spam Act,* the *Do Not Call Register Act* and the *Privacy Act* may cause difficulties for businesses seeking to comply with the Acts.[145] Some stakeholders have also noted that the *Spam Act* and the *Do Not Call Register Act* regulate activities affecting account-holders, while the *Privacy Act* regulates activities affecting individuals.[146] The ALRC is interested in hearing whether the interaction between the *Privacy Act*, the *Spam Act* and the *Do Not Call Register Act* is problematic.

Question 10–1 Do the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) provide adequate and effective protection for the use, disclosure and storage of personal information?

Question 10–2 What issues, if any, are raised by the interaction between the *Privacy Act* and the following Acts:

- *Telecommunications Act 1997* (Cth);
- *Telecommunications (Interception and Access) Act 1979* (Cth);
- *Spam Act 2003* (Cth);
- *Do Not Call Register Act 2006* (Cth)?

Are there acts and practices regulated by these Acts that would be dealt with better under the *Privacy Act*?

144 Australian Government Department of Communications Information Technology and the Arts, *Do Not Call Register Web Page* <www.dcita.gov.au/tel/do_not_call> at 8 August 2006.

145 Privacy Professionals, *Consultation PM 11*, Sydney, 3 August 2006; Australian Direct Marketing Association, *Consultation PC 30*, Sydney, 30 May 2006.

146 Law Council of Australia Privacy Working Group, *Consultation PC 32*, Sydney, 12 July 2006; Australian Direct Marketing Association, *Consultation PC 30*, Sydney, 30 May 2006.

Question 10–3 What bodies (public or private) should be involved in the regulation of personal information in the telecommunications industry?

11. Developing Technology

Contents

Introduction

11.1 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

1 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.
2 D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 10.
3 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), Rec 58.

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 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]

11.2 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]

11.3 This chapter examines the impact of a number of new technologies on privacy. It commences by providing a brief overview of these technologies. It then considers the ability of the *Privacy Act* to protect personal information in light of these technologies. It is important to note at the outset that there are some technologies that operate to protect privacy. These are known as 'privacy enhancing technologies' (PETs). While these are discussed at various points throughout the chapter, they are not examined in detail.

The impact of developing technology on privacy

The internet

11.4 The internet is a worldwide collection of interconnected computer networks based on a common addressing system and communications protocol. The World Wide Web (the Web)—a large collection of publicly accessible information—can be accessed via the internet. The internet was created in the mid 1980s and widespread use of it commenced in the 1990s. In 2004, 65% of respondents to a survey conducted by Roy Morgan Research for the OPC indicated that they used the internet at least once a week.[7] In 2005, it was estimated that 68.2% of the Australian population used the internet.[8]

---

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 Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (2004), [10.1].

8 Internet World Stats, *Australia: Internet Usage Stats and Telecommunications Market Report* <www.internetworldstats.com/sp/au.htm> at 12 September 2006.

11.5 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.

11.6 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.[9] Data are also collected about internet users who use tools provided by online search engines, such as free email and map services.[10] 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'.[11] 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 has a unique Internet Protocol (IP) address.[12]

11.7 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.[13] Two in three respondents indicated that they had more concerns about their privacy when using the internet than they did two years previously.[14]

11.8 This section provides a brief overview of the way in which data can be collected about internet users. It then examines other ways in which use of the internet can impact on privacy.

Cookies

11.9 A 'cookie' is a piece of information that is sent from a 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

---

9 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 113.
10 See, eg, A Brown, 'Google is Watching …', *The Age* (Melbourne), 2 September 2006, Insight 3.
11 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 114.
12 G Greenleaf, 'Privacy Principles—Irrelevant to Cyberspace?' (1996) 3 *Privacy Law & Policy Reporter* 114, 115.
13 Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (2004), [10.2].
14 Ibid, [10.2].

user's computer to the website, thereby indicating that the same user has returned to the same website.

11.10 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 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.

11.11 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 set the browser cookie file to 'read only', which will limit the lifespan of cookies so that they are only stored for as long as the 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

11.12 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.

11.13 When an email containing a web bug is accessed, 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.[15]

Hypertext Transfer Protocol (HTTP)

11.14 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. However, further information can also be sent during the request for information, such as the email address of the internet user, or the last web page viewed by the user.[16] If the last web page viewed by the user was an online search

15 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 118.

16 Office of the Privacy Commissioner, *Protecting your Privacy on the Internet* <www.privacy.gov.au/internet> at 12 September 2006.

engine, then the search term entered is also transmitted.[17] 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.[18]

Spyware

11.15 Spyware is software installed on a computer that enables a third party to view the activity or data on a computer.[19] Spyware is not inherently harmful. It could be used, for example, by an employee in a large organisation to fix another employee's computer from a remote location. Spyware can, however, 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.

11.16 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 if, for example, it is 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).[20]

Other privacy issues

11.17 Another major concern about privacy and the internet relates to the content of information published on the Web. The content of some websites may be privacy-invasive. For example, it has been estimated that there are at least 100 websites that contain images of people caught showering or undressing.[21] Currently, a procedure exists for removing offensive or illegal content that is accessible via the internet.[22] However, there is no similar procedure for removing other privacy-invasive information published on the Web by an individual acting in his or her non-business capacity. This type of activity does not amount to an interference with privacy under the *Privacy Act*.

---

17 Y Lim, *Cyberspace Law: Commentaries and Materials* (2002), 119.

18 Ibid, 119.

19 Australian Government Department of Communications Information Technology and the Arts, *Spyware Discussion Paper* (2005), [2.2.2].

20 Australian Government Department of Communications Information Technology and the Arts, *Outcome of the Review of the Legislative Framework on Spyware* (2005), [2.3].

21 C Calvert, *Voyeur Nation: Media, Privacy, and Peering in Modern Culture* (2000), cited in D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 100.

22 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.

11.18 In August 2005, the Standing Committee of Attorneys-General released a discussion paper on the unauthorised publishing of photographs on the Web.[23] It noted that the small size of cameras and the advent of mobile telephone cameras increased the ease with which photographs could be taken of others without their knowledge or consent.[24] It also noted that the unauthorised publishing of photographs on the Web highlighted a tension between privacy and freedom of expression.[25] Several options for reform were suggested, including criminalising the unauthorised publishing of photographs of children on the Web.[26]

11.19 Further, there is a 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.

11.20 Finally, there is a concern about anonymity during online transactions. It has been noted that 'an important aspect of privacy is allowing individuals to have some control over when and to what extent they identify themselves'.[27] The remote nature of online transactions has led many businesses engaged in e-commerce to require individuals to authenticate their identity during transactions as a matter of routine. It is arguable, however, that it is not always necessary for individuals to identify themselves when engaging in online transactions and that it is more desirable for some forms of transactions to be 'pseudonymous'.[28] A pseudonymous transaction 'is one that cannot, in the normal course of events, be associated with a particular individual'.[29] 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 that enables him or her to conduct transactions with other third parties.[30]

11.21 Concerns about privacy in the online environment have led to the development of a number of PETs that can be deployed by internet users. For example, the Privacy for Platform Preferences (P3P) is a technical standard that allows a user to pre-determine the information he or she is willing to part with in the online environment and the information that he or she wishes to be able to access in the online

---

23 Standing Committee of Attorneys-General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (2005).

24 Ibid, [26].

25 Ibid, [21].

26 Ibid, [6.1.1]–[6.2.2].

27 M Crompton, 'Under the Gaze, Privacy Identity and New Technology' (Paper presented at International Association of Lawyers 75th Anniversary Congress, Sydney, 28 October 2002).

28 D Giles, *Consultation PC 6*, Sydney, 2 March 2006.

29 R Clarke, *Identified, Anonymous and Pseudonymous Transactions: The Spectrum of Choice* (1999) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/UIPP99.html> at 12 September 2006.

30 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 13 September 2006.

environment.[31] In addition, encryption can be used to convert data to a form in which they cannot be read without using an appropriate 'key'. It also enables the 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.[32]

Regulating the privacy of internet users

11.22 The Internet Industry Association (IIA) is of 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.[33] 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'.[34]

11.23 In 2003, the IIA lodged a draft privacy code with the OPC for approval under s 18BB of the *Privacy Act*.[35] 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.[36]

11.24 The code aims to close a number of gaps in the existing privacy regime. Accordingly, it may apply to small business operators who are currently exempt from the operation of the *Privacy Act*. It may also apply when personal information is included in an employee record or is collected for inclusion in a generally available publication.[37] However, the code does not apply to individuals dealing with personal information in their personal capacity.[38]

Voice over Internet Protocol (VoIP)

11.25 Voice over Internet Protocol (VoIP) enables spoken conversations to be conducted in real time over the internet.[39] It is a subset of technology referred to as 'IP Telephony', which enables facsimile messages, video and other forms of data

---

31 Parliament of Australia—Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society* (2000), [2.131]–[2.135]. See also R Clarke, *Platform for Privacy Preferences: An Overview* (1998) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html> at 12 September 2006.

32 Parliament of Australia—Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society* (2000), [2.77]–[2.113].

33 Internet Industry Association, *What is Co-regulation?* (1998) <www.iia.net.au> at 12 September 2006.

34 Ibid.

35 Privacy codes are discussed further in Ch 6.

36 Internet Industry Association, *Internet Industry Privacy Code of Practice: Consultation Draft 1.0* (2001).

37 Ibid.

38 Ibid.

39 For example, Skype software enables users to access VoIP services.

traditionally transmitted via the Public Switched Telephone Network (PSTN) to be transmitted via the internet.

11.26 VoIP technology transmits the sound waves of speech via the internet in the form of IP data packets.[40] 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.[41] Alternatively, VoIP technology can offer 'any-to-any connectivity' services, allowing users to make and receive calls to and from any telephone number.[42]

11.27 VoIP services will usually be classified as carriage services for the purposes of the *Telecommunications Act 1997* (Cth).[43] 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 Chapter 10. However, if a VoIP service does not connect with the PSTN at all the service provider may not be regulated by the *Telecommunications Act 1997* but may be regulated by the *Privacy Act.*[44]

11.28 A concern that has arisen in relation to VoIP technology is that Australians may access voice services from providers outside Australia.[45] This may impact on the standards of protection for personal information disclosed during a VoIP call.[46] The OPC Review recommended that the Australian Government consider initiating discussions in international forums about methods to deal with international jurisdictional issues arising from the global reach of new technologies such as VoIP.[47]

Smart cards

11.29 A smart card is a plastic card with an embedded microchip that can be programmed to perform multiple and varied functions.[48] A microchip embedded in a

---

40 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.

41 Ibid, 14–15.

42 Ibid, 15.

43 Ibid, 19.

44 J Malcolm, 'Privacy Issues with VoIP telephony' (2005) 2 *Privacy Law Bulletin* 25, 26.

45 Ibid, 25.

46 Ibid, 25.

47 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.

48 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.

smart card can vary in sophistication.[49] Some microchips have memory functions only, while others have a 'a micro-controller, various types of memory and an operating system'.[50] 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'.[51]

11.30 Smart card technology has existed for several decades and has been described as 'technology looking for an application'.[52] Currently, smart card technology has a number of established uses. For example, a Subscriber Identity Module (SIM) card in a mobile telephone uses smart card technology.[53] 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.[54]

11.31 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. However, a contactless smart cards uses low-frequency radio waves to communicate with readers. Accordingly, they can be read from a distance.[55]

11.32 The use of smart card technology raises several privacy concerns. One concern is that a particular smart card will often be able to be linked to a particular individual. For example, a smart card may be linked to an individual if 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 indentifiable individuals may mean that individuals no longer have the option of transacting anonymously.[56] 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

---

49 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006), [b.6].
50 Ibid, [b.6].
51 Ibid, [b.6].
52 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), 3.
53 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.
54 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), i.
55 Council of Europe, *Report on the Protection of Personal Data with Regard to the Use of Smart Cards* (2001).
56 Privacy Committee of New South Wales, *Smart Cards: Big Brother's Little Helpers* (1995), ii.

> 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.[57]

11.33 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 better market goods and services to them. They may also be sought by third parties, such as law enforcement agencies.[58]

11.34 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, dislosure, accuracy and security of personal information collected by the smart card system.[59] Concern has also been expressed about the security of information stored on smart cards and in smart card systems; the potential for function creep and smart card systems;[60] and the ability to read contactless smart cards without the cardholder's knowledge or consent.

11.35 In 2004, the Council of Europe published a set of guiding principles for the protection of personal information in systems using smart card technology.[61] 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.

11.36 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'.[62] 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.[63] Further, they require a data subject to be alerted every time personal information is exchanged between a smart card and a smart card system.[64]

11.37 In 2006, the Australian Government released part of a framework to assist agencies seeking to implement smart card technology.[65] 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

---

57 Ibid, ii.
58 Ibid, ii–iii.
59 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].
60 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].
61 Council of Europe, *Guiding Principles for the Protection of Personal Data with Regard to Smart Cards* (2004).
62 Ibid, Principle 2.
63 Ibid, Principle 6.
64 Ibid, Principle 9.
65 Australian Government Information Management Office, *Australian Government Smartcard Framework* (2006).

privacy impact assessments to be undertaken 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'.[66]

Biometrics

11.38 Biometric technologies enable unique behavioural or physiological attributes of people to be used for identification and authentication.[67] Major biometric technologies include finger scanning, hand geometry, facial recognition, iris and retinal scanning, finger geometry, voice recognition and dynamic signature verification.[68] Other biometric technologies include ear geometry, body odour measurement, keystroke dynamics and gait recognition.[69]

11.39 In a typical biometric system, a biometric device, such as a finger scanner, is used to take a biometric sample from an individual.[70] 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.[71] Later biometric samples taken from the individual can then be compared to the stored biometric information to determine who the individual is (one-to-many matching) or to attempt to verify that an individual is who he or she claims to be (one-to-one matching).[72]

11.40 Biometric technologies have existed for decades.[73] However, the use of biometric technologies is increasing because of globalisation, developments in information technology, and the desire to identify individuals in order to manage security threats such as terrorism.[74] Biometric systems enable the identitification of an individual to be ascertained or authenticated with a high 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'.[75] For this reason, biometric technologies are increasingly used in

66 Ibid, [a.17].
67 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].
68 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.
69 Ibid, 4.
70 Ibid, 17.
71 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.
72 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 17.
73 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [8].
74 Ibid, [12].
75 Ibid, [8].

identification systems, along with other passwords or identity objects, such as smart cards.[76]

11.41 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.[77] 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.[78]

11.42 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.[79] 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.[80] 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.[81] 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.[82] Australian ePassport holders will also be able to participate in the United States Visa Waiver Program.[83]

11.43 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.[84]

---

76 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 13–14.

77 European Commission, *EURODAC: The Fingerprint Database to Assist the Asylum Procedure* (2004).

78 International Civil Aviation Organization, *ICAO Recommendation* <www.icao.int/mrtd/biometrics/recommendation.cfm> at 4 September 2006.

79 *Migration Act 1958* (Cth) ss 5A, 40, 46, 166, 170, 172, 175, 188, 192.

80 Explanatory Memorandum, Migration Legislation Amendment (Identification and Authentication) Bill 2003 (Cth).

81 A Downer (Minister for Foreign Affairs), 'Australia Launches ePassports' (Press Release, 25 October 2005).

82 Australian Customs Service, *SmartGate* (2006) <www.customs.gov.au/site/page.cfm?u=4243> at 4 September 2006.

83 United States Government Department of State, *Visa Waiver Program (VWP)* (2006) <travel.state.gov/visa/temp/without/without_1990.html> at 4 September 2006.

84 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 240.

11.44 The Council of Europe has cautioned that biometric systems should not be implemented for the mere sake of convenience.[85] 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.[86]

11.45 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.[87] However, some general concerns are as follows.

11.46 First, there is a concern that widespread use of biometric systems will enable extensive monitoring of the activities of individuals.[88] 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.[89] Secondly, there is a concern that biometric technologies, such as facial recognition technologies, may be used to identify individuals without their knowledge or consent.[90] Thirdly, there is a concern biometric information could reveal sensitive personal information, such as information about a person's health or religious beliefs.[91] 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.[92] Finally, the accuracy and reliability of many biometric systems are still unknown,[93] causing some to express concern about the serious

---

85 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [107].

86 Ibid, [107].

87 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).

88 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12.

89 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 12.

90 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 12–13.

91 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).

92 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 13–15.

93 Ibid, 36.

consequences for an individual who is falsely accepted or rejected by a biometric system.[94]

11.47 On 27 July 2006, the Privacy Commissioner announced the approval of the *Biometrics Institute Privacy Code*.[95] 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'.[96] The Code is binding on Biometrics Institute members who sign the Biometrics Institute Privacy Code Agreement to Comply.[97] To date, two organisations have agreed to be bound by the Code.[98]

11.48 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 National Privacy Principles (NPPs); and (iii) promote biometrics as PETs.[99] It includes information privacy standards that are at least equivalent to the NPPs.[100] 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.[101]

11.49 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. In addition, it mandates the use of privacy impact assessments as part of the planning and management process for biometrics implementation.

---

94 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.

95 K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

96 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), Preamble, [2].

97 Ibid, [C.1], [C.2].

98 Biometrics Institute, *Biometrics Institute Privacy Code—Public Register* (2006) <www.biometricsinstitute.org> at 4 September 2006.

99 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [B.1].

100 K Curtis (Privacy Commissioner), 'Privacy Commissioner Approves Biometrics Institute Privacy Code' (Press Release, 27 July 2006).

101 Biometrics Institute, *Biometrics Institute Privacy Code* (2006), [D.5].

DNA-based technologies

11.50 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.[102] However, the use of DNA-based technologies raise a number of the same privacy issues as are raised by the use of biometric technologies.

Genetic samples

11.51 In 2003, the ALRC and the Australian Health Ethics Committee of the National Health and Medical Research Council (AHEC) 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 8.

11.52 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.[103] This meant that these types of samples could be collected, stored and transferred with little or no regulation.

11.53 ALRC 96 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.[104]

11.54 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.[105]

---

102 Organisation for Economic Co-operation and Development, *Biometric-Based Technologies* (2004), 4.

103 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].

104 Ibid, Rec 8–2.

105 Ibid, Rec 8–3.

11.55 In addition, 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.[106] The Australian Government rejected these recommendations and, to date, they have not been implemented.[107] The ALRC does not propose to revisit these issues in the current Inquiry.

Radio Frequency Identification (RFID)

11.56 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.[108] 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.[109] Once data is collected by a reader it is sent to a 'back office'—namely, a data processing system.[110]

11.57 There are two main types of RFID tags—passive tags and active tags.[111] Passive tags lack an internal power source and can only operate if they are in range of a reader that activates the tag.[112] Accordingly, they have a limited 'read range'. However, they are relatively inexpensive and have a longer life-cycle than active tags.[113] Active tags have an internal power source (usually a battery) that allows them to emit radio waves.[114] 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

106 Ibid, Rec 8–4.

107 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 2 August 2006.

108 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

109 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].

110 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

111 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].

112 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

113 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].

114 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

kilometres)[115] and active tags have larger amounts of memory and better processing capabilities than passive tags.[116]

11.58 RFID tags can be attached to objects, such as clothes, shopping trolleys or plastic cards. They can also be attached to animals and people. 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 about unconscious patients.[117] 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 puchase of a product.[118] 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.[119]

11.59 RFID technology has been in existance since the 1940s.[120] 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.[121] Additional uses for RFID technology are being deployed as the cost of the technology decreases.[122] 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.[123]

11.60 The use of RFID technology can benefit businesses, individuals and governments.[124] For example, it can be used by businesses to track products from the point of manufacture to the point of sale, thereby reducing inventory and labor costs, and stock losses.[125] Other applications of RFID technology include:

---

115 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].

116 Ibid, [2.1].

117 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.133]–[3.143].

118 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

119 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.

120 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 7.

121 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.

122 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 August 2006.

123 IDTechEx, *RFID Market $2.77Bn in 2006 to $12.35Bn in 2010* <www.idtechex.com> at 30 August 2006.

124 European Commission Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP105 (2005), [1].

125 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.

> 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 labeling for monitoring of location, expiration and anti-counterfeiting.[126]

11.61 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.[127]

11.62 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.[128]

11.63 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 has been collected.[129] Technologies have been developed that aim to prevent the unwanted scanning of RFID tags, such as the 'blocker tags' which 'impair readers by simulating the signals of many different RFID tags'.[130] However, it has been argued that PETs are unable completely to 'assuage the danger to privacy engendered by RFID technology'.[131]

11.64 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;

---

126 G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 307–308.

127 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 8.

128 European Commission Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP105 (2005), [1].

129 Organisation for Economic Co-operation and Development, *Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations* (2006), 5.

130 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.

131 G Eschet, 'FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification' (2005) 45 *Jurimetrics* 301, 320.

- 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.[132]

11.65 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.[133]

11.66 In 2003, data protection and privacy commissioners from around the world adopted a resolution calling for the basic principles of data protection and privacy law to be observed when designing, implementing and using RFID technology.[134] Also in 2003, a number of consumer and civil liberties groups jointly issued a position statement on the use of RFID. The statement, among other things, listed practices relating to the use of RFID technology that should be prohibited. These included tracking of individuals directly or indirectly through items in their possession and using RFID technology to reduce anonymity by, for example, incorporating RFID tags into currency.[135]

11.67 In January 2005, the European Union Data Protection Working Party[136] released a public consultation document on data protection and the use of RFID technology that contained guidelines on the application of EU data protection legislation to information

---

132 S Garfinkel, 'An RFID Bill of Rights 1' (2002) 105(8) *Technology Review* 35, 35.

133 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 August 2006.

134 Office of the Privacy Commissioner, 'World's Privacy Regulators Call for Privacy Friendly RFID Tags' (Press Release, 9 December 2003).

135 Privacy Rights Clearinghouse, *RFID Position Statement of Consumer, Privacy and Civil Liberties Organizations* (2003) <www.privacyrights.org> at 30 August 2006.

136 This working party was established by art 29 of 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*, Directive 95/46/EC (1995).

collected through RFID technology.[137] Responses to the consultation document varied. Most businesses (except for those that provided security solutions) were of the view that the EU Directive adequately protected personal information collected through the use of RFID technology. On the other hand, most individuals, universities and 'think tanks' were of the view that additional legislation or guidance was required to protect personal information collected through the use of RFID technology.[138] The European Commission is currently conducting consultations about the use of RFID technology with a view to preparing by the end of 2006 a Communication to the Council and the European Parliament on RFID.[139]

Wireless technologies

11.68 Wireless technologies enable devices to trasmit and receive data 'by means of a signal that uses some part of the electromagnetic spectrum'.[140] RFID technology, discussed above, is a wireless technology. 'WiFi' and 'Bluetooth' are examples of other wireless technologies.[141] 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.

11.69 Wireless technologies can be used to purchase goods, services or digital content (m-commerce),[142] to enhance business performance (m-enterprise)[143] and to provide services that do not involve commercial transactions, such as mobile banking services (m-services).[144] 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'.[145] Further, devices that use wireless technologies, such as laptop computers and mobile telephones, are vulnerable to theft and subsequent misuse.

Location detection technologies

11.70 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

137 European Commission Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP105 (2005).

138 Ibid.

139 European Commission, *Your Voice on RFID: Background Document for Public Consultation on Radio Frequency Identification (RFID)* (2006), 4.

140 R Clarke, *Wireless Transmission and Mobile Technologies* (2003) Australian National University <www.anu.edu.au/people/Roger.Clarke/EC/WMT.html> at 7 September 2006.

141 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.

142 C Gould and others, *Mapping the Mobile Landscape in Australia* (2006) Unpublished Working Paper of the Smart Internet Technology Cooperative Research Centre, 8–10.

143 Ibid, 10–13.

144 Ibid, 13–14.

145 Ibid, 6.

be located include mobile telephones, laptop computers, personal digital assistants and gaming consoles.[146]

11.71 The accuracy of location information may vary depending on the location detection technology used. For example, the global positioning system (GPS) can be used to determine the location of a device with a high degree of accuracy if the device contains a GPS receiver. The GPS is a network of 24 satellites established and operated by the United States Department of Defense.[147] 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.[148] 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.[149] 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.[150]

11.72 Location detection technologies and other wireless technologies allow 'location-based services' to be provided to individuals.[151] 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.[152]

11.73 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.[153] However, they are unable to determine accurately the location of users of mobile telephones.[154] 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.[155]

---

146 S Benford, *Future Location-Based Experiences* (2005) Joint Information Systems Committee Technology and Standards Watch, 4.

147 Australian Communications Authority, *Location Location Location* (2004), 32.

148 Ibid, 32.

149 Ibid, 33.

150 Ibid, 31, 34.

151 S Benford, *Future Location-Based Experiences* (2005) Joint Information Systems Committee Technology and Standards Watch, 4.

152 See, eg, Ibid, 4; M James, *Where are You Now? Location Detection Systems and Personal Privacy* (2004) Parliamentary Library—Parliament of Australia.

153 Australian Communications Authority, *Location Location Location* (2004), 17. The Integrated Public Number Database is discussed in Ch 10.

154 Ibid, 18.

155 See Federal Communications Commission, *Enhanced 911–Wireless Services* (2006) <www.fcc.gov/911/enhanced/> at 7 September 2006.

11.74 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 the individual's consumer preferences or social activities.

11.75 The European Union Directive on Privacy and Electronic Communications deals explicitly with 'location data' in the electronic communications sector.[156] 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'.[157] The Directive prohibits the processing of location data that has not been anonymised without the consent of the user of the service.[158] It also requires service providers to inform users, prior to obtaining their 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.[159] Users must be given the opportunity to withdraw their consent at any time to the processing of location data.[160] Further, processing of the data must be restricted to that which is necessary for the purposes of providing the value added service.[161]

Data-matching and 'data mining'

11.76 Rapid advances in information and communications 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 every day 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 or an insurance claim; and, increasingly, sending or receving e-mail and surfing the Net.[162]

11.77 In addition, technologies have been developed that 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.

---

156 European Parliament, *Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector*, Directive 2002/58/EC (2002).
157 Ibid, art 2.
158 Ibid, art 9(1).
159 Ibid, art 9(1).
160 Ibid, art 9(1), (2).
161 Ibid, art 9(3).
162 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 1.

11.78 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'.[163] Developments in information technology in the 1970s made data-matching economically feasible and it is currently conducted regularly in Australia, particularly by government agencies.[164] Data-matching can be conducted for a number of purposes, including to detect errors and illegal behaviour, to locate individuals, to ascertain whether a particular individual is eligible to receive a benefit, and to facilitate debt collection.[165]

11.79 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 ensure that any adverse effects of such developments on privacy are minimised.[166] 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.[167] The Privacy Commissioner may report to the Minister (currently the Attorney-General)[168] about the results of any research into developments in data-matching or proposals for data-matching.[169]

11.80 As discussed in Chapters 7 and 12, the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the *Data-matching Program (Assistance and Tax) 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. For example, the Privacy Commissioner provides advice to agencies about the interpretation of the Act and inspects the way in which they undertake data-matching regulated by the Act.[170] An act or practice that breaches Part 2 of the *Data-matching Program (Assistance and Tax) Act 1990* (Cth), or the Guidelines, constitutes an 'interference with privacy'.[171] An individual can complain to the Privacy Commissioner about any such act or practice.[172]

---

163 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [14].

164 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.

165 Ibid, 33.

166 *Privacy Act 1988* (Cth) s 27(1)(c).

167 Ibid s 27(1)(k).

168 Commonwealth of Australia, *Administrative Arrangements Order*, 16 December 2004, pt 2.

169 *Privacy Act 1988* (Cth) ss 27(1)(c), 32(1).

170 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), [3.8].

171 *Privacy Act 1988* (Cth) s 13.

172 Ibid s 36; *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 14.

11.81 Agencies may also engage in data-matching activities that do not involve the use of tax file numbers. For example, in early 2004 the Australian Securities and Investments Commission began matching data from its public database with data from the Insolvency and Trustee Service Australia's National Personal Insolvency Index.[173] The purpose of this data-matching program is to identify individuals who should be automatically disqualified from managing corporations under the *Corporations Act 2001* (Cth).[174]

11.82 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).[175] The guidelines aim to ensure that data-matching programs 'are designed and conducted in accordance with sound privacy practices'.[176] Although the guidelines are not legally binding, a number of agencies have agreed to comply with them.[177]

11.83 The 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.[178] In summary, the guidelines require agencies to give public notice of any proposed data-matching program;[179] to prepare and publish a 'program protocol' outlining the nature and scope of a data-matching program;[180] to provide individuals with an oportunity to comment on matched information if the agency proposes to take administrative action on the basis of it;[181] and to destroy personal information that does not lead to a match.[182] Further, the guidelines generally prohibit agencies from creating new, separate databases from information about individuals whose records have been matched.[183]

11.84 Data mining has been defined as 'a set of automated techniques used to extract buried or previously unknown pieces of information from large databases'.[184] Data

---

173 Australian Securities and Investments Commission, *ITSA Data Matching Protocol* <www.asic.gov.au> at 6 September 2006.

174 Ibid.

175 Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997).

176 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), 1.

177 Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2003–30 June 2004* (2004), 69–70.

178 Office of the Federal Privacy Commissioner, *The Use of Data Matching in Commonwealth Administration—Guidelines* (1998), [15].

179 Ibid, [33]–[41].

180 Ibid, [42]–[47].

181 Ibid, [63].

182 Ibid, [69].

183 However, this does not prevent the creation of a register of individuals who warrant further investigation, or of a register to exclude individuals from being selected for investigation in successive cycles of the data-matching program: Ibid, [72]–[75].

184 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 4.

mining can be used in different contexts to achieve different goals.[185] 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'.[186] Data mining can also be used by law enforcement agencies to investigate criminal activities. For example, in 2006 it became apparant 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.[187]

11.85 There are three main steps in the data-mining process. First, the data are prepared (or 'scrubbed') for use in the data-mining process. Secondly, a data-mining algorithm is used to process the data, and finally the results of the data-mining process are evaluated.[188]

11.86 Data-matching and data-mining practices that involve personal information raise privacy concerns. A major concern is that the practices can reveal large amounts of previously unknown personal information about individuals.[189] 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.[190]

11.87 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.[191] 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

185 Electronic Privacy Information Centre, *Submission to the United States House Government Reform Committee on Data Mining: Current Applications and Future Possibilities*, 25 March 2003.

186 Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 1.

187 L Cauley, 'NSA has Massive Database of Americans' Phone Calls', *USA Today*, 10 May 2006, <www.usatoday.com>.

188 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.

189 V Estivill-Castro, L Brankovic and D Dowe, 'Privacy in Data Mining' (1999) 6 *Privacy Law & Policy Reporter* 33, 34.

190 See, eg, Information and Privacy Commissioner Ontario, *Data Mining: Staking a Claim on Your Privacy* (1998), 14.

191 See, eg, Ibid, 10–11.

discover previously unknown information. Further, there is concern about the storage of large amounts of personal information gathered for the purpose of data mining.[192]

Surveillance technologies

11.88 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.[193] 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'.[194] While surveillance is said to be 'at least as old as recorded history',[195] developments in surveillance technology and the increased availability of this technology pose significant risks to privacy.

11.89 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.[196] Accordingly, it recommended that legislation prohibit the use of listening devices for non-consensual or secret surveillance,[197] with some exceptions for the use of listening devices for law enforcement purposes and for 'participant monitoring'.[198]

11.90 ALRC 22 also considered the use of optical surveillance devices. The ALRC noted that the 'growth and increased sophistication of modern technological surveillance devices make it imperative that some legislative control be imposed on their use for optical surveillance'.[199] 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.[200] 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.[201]

---

192 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 240.

193 R Clarke, *Have We Learnt to Love Big Brother?* (2005) Australian National University <www.anu.edu.au/people/Roger.Clarke/DV/DV2005.html> at 11 September 2006.

194 New South Wales Law Reform Commission, *Surveillance: An Interim Report*, Report 98 (2001), [1.5].

195 Ibid, [1.18].

196 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983), [1122].

197 Ibid, Recs 28, 30.

198 Ibid, Recs 29, 40–50. Participant monitoring is discussed in Ch 1.

199 Ibid, [1187].

200 Ibid, Recs 52–53.

201 Ibid, Recs 53–54.

11.91 There are ceaseless 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.[202] 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.[203] Intelligent software can reduce the need for live monitoring of surveillance systems and reduce costs associated with recording irrelevant activity.[204]

11.92 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.[205] Generally, federal law enforcement officers must obtain a warrant to use a surveillance device. 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.[206] In addition, a listening device can be used without a warrant if an officer is participating in the conversation.[207] The use of surveillance devices by the Australian Security Intelligence Organisation (ASIO) is regulated by the *Australian Security Intelligence Organisation Act 1979* (Cth), while the intelligence gathering functions of the Australian Security Intelligence Service (ASIS) and the Defence Signals Directorate (DSD) are set out in the *Intelligence Services Act 2001* (Cth).

11.93 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.

---

202 Council of Australian Governments, *A National Approach to Closed Circuit Television*, 14 July 2006, 18.
203 See, eg, T Holding (Victorian Minister for Police and Emergency Services), 'Government to Keep Eye on Number Plate Trial' (Press Release, 16 March 2005).
204 Council of Australian Governments, *A National Approach to Closed Circuit Television*, 14 July 2006, 18.
205 *Surveillance Devices Act 2004* (Cth) s 6(1).
206 Ibid s 37.
207 Ibid s 38.

Publicly available information in electronic form

11.94 Currently, personal information about a substantial number of people is available from sources such as electoral rolls, court records, state registers of births, deaths and marriages, annual reports and newspapers.[208] This information may be of interest to a range of 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. This section provides an overview of two sources of publicly available information—public registers and court records—before examining concerns about the impact of publishing publicly available information electronically.

Public registers

11.95 In the late 19th century governments began systematically to compile and retain records of their citizens.[209] Today, records are kept 'for almost every occasion an individual comes into contact with the state bureaucracy'.[210] 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.[211]

11.96 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'.[212] However, there is a tension between the public interests served by a public register of information and privacy. This is exacerbated when it is compulsory to provide the government with the information that is included in the register.[213]

11.97 It has been argued that failure to protect adequately the privacy of personal information contained in public registers can have serious consequences. For example, individuals may choose to withdraw from public life in order to protect their privacy.[214]

---

208 M Neave, 'International Regulation of the Publication of Publicly Accessible Personal Information' (2003) 10 *Privacy Law & Policy Reporter* 120, 120.

209 D Solove, 'Access and Aggregation: Privacy, Public Records and the Constitution' (2002) 86 *Minnesota Law Review* 1137, 1143.

210 Ibid, 1143.

211 *Commonwealth Electoral Act 1918* (Cth) s 90A.

212 Australian Electoral Commission, *How to View the Commonwealth Electoral Roll* <www.aec.gov.au/_content/what/enrolment/index.htm> at 12 September 2006.

213 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.

214 See B Givens, *Public Records on the Internet: The Privacy Dilemma* (2002) Privacy Rights Clearinghouse <www.privacyrights.org/ar/onlinepubrecs.htm> at 8 September 2006.

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'.[215] 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.[216]

11.98 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.

Court records

11.99 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'.[217] In 2006, the New Zealand Law Commission concluded that the principle of open justice generally required open access to court records.[218]

11.100 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 often include details of the financial circumstances of bankruptees; records of cases in which compensation is sought often include detailed information regarding the health of the plaintiff; and records of family court proceedings often contain detailed information about family relationships. Records of criminal cases may include information about an offender's previous criminal history, social security status or mental health.

11.101 Access to court records is regulated by legislation or rules of court.[219] 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.[220] However, a person who is not a party to the proceeding may only inspect certain documents, such as interrogatories or answers to

---

215 Australian Electoral Commission, *Submission to the Joint Standing Committee on Electoral Matters Inquiry into the 2001 Federal Election*, 1 July 2002, Appendix D, 8.
216 Roy Morgan Research, *Community Attitudes Towards Privacy 2004* (2004), [6.4].
217 New Zealand Law Commission, *Access to Court Records*, Report 93 (2006), [2.2].
218 Ibid, [2.4].
219 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. Public access to court records is discussed further in Ch 5.
220 *Federal Court Rules 1979* (Cth) o 46 r 6(1), (2).

interogatories, with the leave of the court.[221] Leave will usually be granted, however, where a document has been admitted into evidence or read out in open court.[222]

Publication in electronic form

11.102 In the past, individuals seeking to access publicly available information were required to attend the location at which the information was stored, such as a court house,[223] and to expend a considerable amount of time manually searching or copying records. This meant that publicly available information was afforded a degree of de facto privacy protection. However, developments in information technology, 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.[224] 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'.[225]

11.103 Information published in electronic form can be easily accessed, searched, aggregated and analysed. This increases the ability of third parties to combine disparate pieces of personal information about others.[226] Further, 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.

11.104 A number of steps could be taken to protect personal information contained in publicly available information that is published electronically. For example, 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.[227] Alternatively, unnecessary personal information could be removed from documents before they are published electronically. Another option is to restict the use and disclosure of publicly available information in electronic form to that which is consistent with the public interest that is served by the publishing of the information.

Other developing technologies

11.105 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

---

221 Ibid o 46 r 6(3), (5).
222 Federal Court of Australia, *Public Access to Court Documents* <www.fedcourt.gov.au> at 21 July 2006.
223 D Solove, 'Access and Aggregation: Privacy, Public Records and the Constitution' (2002) 86 *Minnesota Law Review* 1137, [1152].
224 Ibid, [1152]–[1153].
225 Ibid, [1178].
226 M Neave, 'International Regulation of the Publication of Publicly Accessible Personal Information' (2003) 10 *Privacy Law & Policy Reporter* 120, 122.
227 B Givens, *Public Records on the Internet: The Privacy Dilemma* (2002) Privacy Rights Clearinghouse <www.privacyrights.org/ar/onlinepubrecs.htm> at 8 September 2006.

track others.[228] 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'.[229] In summary, ENUM enables telephones connected to the internet to make calls to the Public Switched Telephone Network and receive calls from the Public Switched Telephone Network.[230]

11.106 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.[231] It has been noted that virtually all DRM technologies require the collection of personal information about consumers of copyright material.[232] Accordingly, they limit the ability of these consumers to access material anonymously.

11.107 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, and the location of use'.[233] 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.[234] 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.[235]

11.108 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. The ALRC is interested in hearing about other technologies that may impact on privacy.

---

228 R Clarke, 'ENUM—A Case Study in Social Irresponsibility' (2003) 9 *Privacy Law & Policy Reporter* 181, 181.

229 Australian Communications Authority, *Annual Report 2004–05* (2005), 36.

230 Australian Communications and Media Authority, *What is ENUM or Electronic Number Mapping?* <www.acma.gov.au/> at 8 September 2006.

231 Information and Privacy Commissioner Ontario, *Privacy and Digital Rights Management (DRM): An Oxymoron?* (2002), 2.

232 Ibid, 4.

233 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).

234 *Australia-US Free Trade Agreement*, 18 May 2004, [2005] ATS 1, (entered into force generally on 1 January 2005), art 17.4.7.

235 Australian Government Attorney-General's Department, *Exposure Drafts—Copyright Amendment (Technological Protection Measures) Bill 2006 and related Regulations* <www.ag.gov.au> at 19 September 2006.

The *Privacy Act* and developing technology

Scope of the *Privacy Act*

11.109 As discussed in other chapters, the *Privacy Act* has limited application. First, the Act applies only to Australian Government and ACT public sector agencies and private sector organisations. It does not regulate the activities of state or other territory agencies. Nor does it regulate the handling of personal information by individuals for the purposes of, or in connection with, their personal, family or household affairs.[236]

11.110 Secondly, the IPPs and NPPs apply only when personal information is held, or collected for, inclusion in a 'record'.[237] A record is defined as a document, a database, or a photograph or other pictorial representation.[238] A book, magazine or other publication that is generally available to the public is not a record for the purposes of the *Privacy Act*.[239] Finally, the application of the *Privacy Act* is limited by a number of exemptions. Exemptions are provisions excusing an agency or organisation from complying with specific privacy principles in certain circumstances.

11.111 There are concerns about the limited application of the *Privacy Act* given developments in technology. For example, there is a concern about the use of privacy-invasive technologies by individuals in their non-business capacity. Individuals can now publish large amounts of personal information about others on the Web. One submission to the Inquiry noted that individuals can publish photographs of others on the internet without their knowledge or consent,[240] while another noted that emails sent to multiple people may disclose to each other the email addresses of all of the recipients.[241] Further, individuals can use scanners to listen to communications sent and received by radio frequencies, monitor the online activities of others through the use of spyware,[242] and take photographs of others using mobile telephones with inbuilt cameras. The OPC Review noted that there was limited support for extending the scope of the *Privacy Act* to apply to the activities of individuals in their personal capacity.[243]

11.112 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 CCTV, are not governed by the *Privacy Act*.[244] It has been argued that consideration should be given to ensuring that agencies or organisations cannot

---

236 *Privacy Act 1988* (Cth) ss 7B(1), 16E.
237 Ibid s 14, IPPs 1–11, s 16B. However, this does not apply to pt III divs 3 and 4 (tax file numbers and credit information) and pt IIIA (credit reporting).
238 Ibid s 6.
239 Ibid s 6.
240 Confidential, *Submission PR 49,* 14 August 2006.
241 J Partridge, *Submission PR 26,* 4 June 2006.
242 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 244.
243 Ibid, 246.
244 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [3.19].

breach the spirit of the *Privacy Act* by avoiding making a record.[245] In addition, the fact that the definition of a record excludes a generally available publication means that IPPs 4–11 and NPPs 2–10 do not apply to personal information in generally available publications.

11.113 Concerns also arise about the handling of personal information by exempt agencies or organisations. For example, it has been argued that some small business operators that are not bound by the *Privacy Act*—for example, ISPs—in fact handle large 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*.[246] In 2005, the OPC Review recommended that the Attorney-General consider using the power under s 6(E) of the *Privacy Act* to prescribe ISPs as businesses to be covered by the Act.[247]

11.114 Further, acts and practices of organisations that are employers are exempt from the *Privacy Act* if they are directly related to the employment relationship and an employee record.[248] The former Privacy Commissioner, Mr Malcolm Crompton, has noted that this exemption could be of concern given developments in biometric technology 'because biometric systems have a number of potential uses in the employment context'.[249]

11.115 In addition, the acts and practices of federal courts that are of a non-administrative nature are exempt from the operation of the *Privacy Act*.[250] This means that the *Privacy Act* will not regulate the collection, use, storage or disclosure of personal information in court records.

The definition of 'personal information'

11.116 As discussed in Chapter 3, the *Privacy Act* is limited in its scope to the protection of personal information. It does not regulate other aspects of privacy, such as bodily privacy, territorial privacy or privacy of communications. Personal information is defined as:

---

245 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.

246 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 56.

247 Ibid, Recs 9, 52.

248 *Privacy Act 1988* (Cth) s 7B(3).

249 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).

250 *I v Commonwealth Agency* [2005] PrivCmrA 6.

> 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.[251]

11.117 An issue is whether this definition of personal information is still adequate and appropriate in light of advances in technology.[252] In some circumstances information such as an individual's 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'. 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'. However, these types of information may enable individuals to be contacted, tracked or profiled. The ALRC is interested in hearing about difficulties applying the definition of personal information in light of developments in technology.

11.118 In 2000, the Senate Select Committee on Information Technologies recommended that information collected through the use of technologies such as cookies and web bugs, which could indirectly identify consumers, be regulated by the *Privacy Act*.[253] It suggested that this could be achieved by amending the definition of personal information in the Act.[254]

11.119 The OPC Review and the Senate Committee privacy inquiry both considered whether the definition of personal information was an impediment to the effective operation of the *Privacy Act*. Responses to this issue were varied. Some were of the view that there was no need to amend the definition of personal information, while others opposed any amendment on the basis that it would increase compliance costs and create inconsistency between Australian information privacy laws and those in other countries.[255] However, the Australian Privacy Foundation was of the view that the definition of personal information should be amended to include information enabling individuals to be contacted,[256] while Electronic Frontiers Australia was of the view that personal information should be defined as

---

251 *Privacy Act 1988* (Cth) s 6.

252 M Crompton and R McKenzie, *Consultation PC 3*, Sydney, 24 February 2006; G Greenleaf, *Consultation PC 5*, Sydney, 28 February 2006.

253 Parliament of Australia—Senate Select Committee on Information Technologies, *Cookie Monsters? Privacy in the Information Society* (2000), Rec 4.

254 Ibid, Rec 4.

255 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 246–248.

256 Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005, 7; Australian Privacy Foundation, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, [58].

> 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.[257]

11.120 The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*s (OECD Guidelines),[258] and the Coucil of Europe *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data* (Council of Europe Convention)[259] define 'personal data' as 'any information relating to an identified or identifiable individual'. Similarly, 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) defines 'personal data' as 'any information relating to an identified or identifiable natural person'.[260] 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.[261]

11.121 In Chapter 3 the ALRC asks whether the definition of personal information in the *Privacy Act* is adequate and appropriate.[262] If the definition should refer to the ability directly or indirectly to identify a person, the ALRC is interested in hearing whether the holder of the information should possess the ability or intention to identify the individual to whom it relates,[263] or whether it is sufficient that a third party would be able to use it to identify the individual to whom it relates.[264]

The definition of 'sensitive information'

11.122 NPP 10 prohibits the collection of sensitive information, except in certain identified circumstances. Sensitive information is health information about an individual; genetic information about an individual; genetic information about an

---

257 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, 20. See also Electronic Frontiers Australia Inc, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 24 February 2005, [135]–[146].

258 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), art 1.

259 *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.

260 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.

261 Ibid, art 2.

262 See Question 3–4.

263 In *Eastweek Publisher Limited v Privacy Commissioner for Personal Data* [2000] HKCA 137, the Court of Appeal of Hong Kong held that for personal data to be collected the data user must 'be compiling information about an identified person or about a person whom the data user *intends or seeks to identify*' (emphasis added).

264 The concepts of 'identifiable', 're-identifiable' and 'non-identifiable' information are discussed in Ch 8.

individual that is or could be predictive of the health of the individual or a genetic relative of the individual; or personal 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.[265]

11.123 NPP 10.1 provides that sensitive information can be collected if the individual has consented; the collection is required by law; 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 consent to the collection, or physically cannot communicate consent to the collection; or the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

11.124 In Chapter 3, the ALRC asks whether the definition of sensitive information is adequate and appropriate.[266] In particular, the ALRC is interested in hearing whether other types of personal information that can be collected using new technologies, such as location information or biometric information, should be included in the definition of 'sensitive information'.

The adequacy of existing information privacy principles

11.125 This section examines the adequacy of the IPPs and the NPPs in the *Privacy Act* in light of developments in technology. It examines aspects of selected information privacy principles that may require modification or amendment to accommodate emerging technologies. The ALRC is interested in hearing whether the content of other information privacy principles makes the principles difficult to apply given advances in technology.

Collection

11.126 Neither the IPPs nor the NPPs require agencies or organisations to obtain an individual's consent before collecting personal information.[267] The ALRC is interested in hearing whether there are categories of personal information that can be collected by new technologies, such as biometric information, that should only be collected by consent. If so, the ALRC is interested in views about whether an individual should be able to refuse to provide consent to the collection of these types of personal information without suffering adverse consequences as a result of the refusal.

11.127 Further, neither the IPPs nor the NPPs expressly require the legitimacy of the collection of personal information to be determined objectively. Instead, the IPPs

---

265 *Privacy Act 1988* (Cth) s 6. The definition of 'health information' is discussed in Ch 8.

266 See Question 3–4.

267 The NPPs do, however, prevent organisations from collecting 'sensitive information' in certain circumstances without consent: *Privacy Act 1988* (Cth) sch 3, NPP 10. They also prevent organisations from using personal information for certain unrelated secondary purposes without an individual's consent: *Privacy Act 1988* (Cth) sch 3, NPP 2.

enable agencies to collect personal information for a lawful purpose directly related to a function or activity of the collector, as long as the collection of personal information is 'necessary for or directly related to that purpose';[268] while the NPPs enable organisations to collect personal information that is necessary for one or more of the organisation's functions or activities.[269] In Chapter 4, the ALRC indicates that it is interested in views about whether the reasonableness of the purpose of collection should be determined by reference to the purposes that a reasonable person would consider appropriate in the circumstances. This may impact on the introduction of systems using certain types of technologies to collect personal information, such as biometric identification systems.

11.128 Another issue is whether the notice requirements in the IPPs and the NPPs are adequate. In particular, the ALRC is interested in whether agencies or organisations that use certain technologies to collect personal information should be required to comply with any additional notice requirements. For example, should agencies or organisations using RFID technology be required to inform individuals how to remove or deactivate an RFID tag embedded in a product? Another question is whether agencies or organisations using biometric systems should 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.[270] Further, the ALRC is interested in hearing whether agencies or organisations should be required to inform individuals of the format in which personal information may be disclosed, for example, whether it will be disclosed in electronic format.

Use and disclosure

11.129 The IPPs require agencies to record uses and disclosures of personal information only where the information is used for certain secondary purposes, such as enforcement of the criminal law.[271] Similarly, the NPPs require organisations to record uses and disclosures of personal information only where it relates to a secondary purpose of law enforcement.[272] In Chapter 4, the ALRC asks in what circumstances agencies or organisations should be required to record their use or disclosure of personal information for a purpose other than the primary purpose.[273] The ALRC is interested in hearing whether agencies or organisations should be required to keep a record of use of personal information for any particular purposes or disclosure of personal information by any particular means.

---

268 *Privacy Act 1988* (Cth) s 14, IPP 1.
269 Ibid sch 3, NPP 1.1.
270 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.
271 *Privacy Act 1988* (Cth) s 14, IPPs 10, 11.
272 See Ibid sch 3, NPP 2.2.
273 See Question 4–10.

Security of personal information

11.130 Both the IPPs and the NPPs require agencies and organisations to take reasonable steps to protect personal information from loss, misuse and unauthorised access, modification or disclosure.[274] 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.[275]

11.131 In its submission to the OPC Review, the former Australian Communications Authority noted that security of transactions was important in m-commerce, particularly when credit card information was sent to an organisation using an unencrypted SMS. It submitted that m-commerce providers should be required to design payment methods that adequately protect consumers personal details, and suggested that this could be achieved by amending NPP 4.1 to state that service providers should ensure the payment mechanisms they establish also protect the personal information of consumers.[276]

Access to personal information

11.132 Both the IPPs and the NPPs provide individuals with a general right to access personal information about them that is held by agencies or organisations.[277] One concern is that some personal information may be stored in a way that makes it difficult to analyse or comprehend. The EU Directive requires personal information to be communicated to an individual in an 'intelligible form'.[278] 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.[279]

Data quality

11.133 The IPPs require agencies to ensure that personal information solicited by a collector is up-to-date and complete and that personal information used by an agency is accurate, up-to-date and complete.[280] The NPPs require organisations to ensure that the personal information collected, used or disclosed is accurate and up-to-date.[281] An

---

274 *Privacy Act 1988* (Cth) s 14, IPP 4; sch 3, NPP 4.1.

275 Office of the Federal Privacy Commissioner, *Security and Personal Information*, Information Sheet 6 (2001), 1.

276 Australian Communications Authority, *Submission to the Office of the Privacy Commissioner Review of the Private Sector Provisions of the Privacy Act 1988*, December 2004, 3.

277 *Privacy Act 1988* (Cth) s 14, IPP 6; sch 3, NPP 6.

278 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).

279 Council of Europe, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data* (2005), [82].

280 *Privacy Act 1988* (Cth) s 14, IPP 3, IPP 8.

281 Ibid sch 3, NPP 3.

issue is whether the existing data quality principles are broad enough to require agencies or organisations using some types of technologies to collect personal information, such as biometric systems, to ensure that the technologies produce accurate and reliable results. If the principles are not broad enough to be applied in this way, the question arises as to whether there is a need to require agencies or organisations to ensure that the technologies they use deliver accurate and reliable results. This may be particularly important if the results generated by these technologies are used for secondary purposes, such as to assist law enforcement bodies.

Anonymity

11.134 NPP 8 requires organisations to give individuals the option of transacting with the organisation anonymously, wherever this is 'lawful and practicable'. The IPPs do not contain a corresponding anonymity principle. In Chapter 4, the ALRC asks whether it would be appropriate to require agencies also to comply with an anonymity principle.[282]

11.135 It has been noted that it is unlikely that organisations that implement systems that do not enable individuals to transact with the organisation anonymously, such as biometric identification systems or transport systems using smart card technology, will be required to comply with NPP 8. This is because it would not be 'practicable' restrospectively to alter such a system to allow for anonymity in transactions.[283]

11.136 This difficulty is compounded by the fact that people have limited ability to challenge the development of systems that will breach NPP 8 given that the Privacy Commissioner can only investigate interferences with privacy.[284] Section 98 of the *Privacy Act* may, however, provide a mechanism to challenge the development of systems that will breach NPP 8. This section enables the Privacy Commissioner or any other person to seek an injunction in the Federal Court of Australia or the Federal Magistrates Court restraining a person from engaging in conduct that would constitute a contravention of the Act.

11.137 One issue for consideration is whether NPP 8 should be amended to require organisations to design systems that will comply with the anonymity principle, or provide individuals with the opportunity of transacting 'pseudonymously' if anonymity is impractical or unlawful.[285]

---

282 See Question 4–30.

283 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).

284 *Privacy Act 1988* (Cth) ss 13, 13A, 36, 40.

285 See Australian Privacy Foundation, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 1 March 2005, 17; G Greenleaf and N Waters, *The Asia-Pacific Privacy Charter, Working Draft 1.0, 3 September 2003* (2003) WorldLII Privacy Law Resources

Additional information privacy principles?

11.138 Another issue is whether additional information privacy principles are required in light of developments in technology. For example, art 15 of the EU Directive deals with automated decision making.[286] Article 15(1) provides as follows:

> 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.

11.139 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.[287] Article 15(1) of the EU Directive reflects concern about the increasing automisation of decisions that affect individuals.[288]

11.140 The OPC Review noted that there may be a need for new NPPs that reflect the need for organisations to allow individuals to choose the kind of identity authentication they wish to use, or to prohibit organisations from engaging in profiling activities without the consent of the individuals being profiled.[289] Further, the Privacy Commissioner has expressed support for organisations to adopt the practice of notifying individuals when a breach of security leads to the disclosure of personal information.[290] This is 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. The ALRC is interested in hearing whether additional information privacy principles are required in light of developments in technology, and, if so, what these principles should be.

Should the *Privacy Act* be technologically neutral?

11.141 As the discussion above indicates, there is a question whether the *Privacy Act* provides adequate and appropriate protection of information privacy in light of developments in technology. As one stakeholder to the Senate Committee privacy inquiry noted, 'both government and industry have had to act outside the framework of

---

<www.worldlii.org/int/other/PrivLRes/2003/1.html> at 11 September 2006, [7]. See also N Waters, *Consultation PC 17*, Sydney, 2 May 2006.

286 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 11 September 2006, [17].

287 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(2).

288 L Bygrave, 'Minding the Machine: Art 15 of the EC Data Protection Directive and Automated Profiling' (2000) 7 *Privacy Law & Policy Reporter* 67, 68.

289 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 253.

290 N Miller, 'Data Leaks Under Review', *The Sydney Morning Herald* (Sydney), 8 August 2006, 27. This issue is discussed further in Ch 4.

the *Privacy Act* in areas like spam and there are gaps opening up in areas like surveillance, biometrics and radiofrequency identification'.[291]

11.142 The ALRC is interested in hearing whether the *Privacy Act* should continue to aim to be technologically neutral. Submissions to the OPC Review and the Senate Committee privacy inquiry were generally supportive of this approach, noting that it prevented the need continually to review the adequacy of the Act to accommodate technological change.[292] However, some have questioned whether it is actually possible to develop technologically neutral principles.[293] For example, it has been argued that the impact of some technologies on privacy is inconceivable until the technologies have actually been invented and deployed.[294]

Other regulatory mechanisms

11.143 The ALRC is also interested in hearing about other ways in which personal information can be protected in light of developments in technology. These could include the introduction of technology-specific legislation, the development of voluntary or binding privacy codes of practice, the development of voluntary or binding guidelines, or the preparation of documents assessing the impact of new technologies on privacy prior to their deployment. These regulatory mechanisms are discussed in detail in Chapters 2 and 6.

Question 11–1 What new technologies, or new uses of existing technologies, will, in the future, impact significantly on privacy? How can such technologies be accommodated in a regulatory framework?

Question 11–2 Should the *Privacy Act* be extended to cover: (a) any acts or practices of individuals relating to their personal, family or household affairs; or (b) exempt agencies or organisations that use certain types of technology or collect certain types of personal information?

Question 11–3 Is there a need to amend the *Privacy Act* in light of technological developments? If so, what amendments are required? For example:

---

291 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005).

292 Ibid, [3.10]–[3.17]; Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 242–244. See also Privacy Commission Victoria, *Consultation PC 20*, Melbourne, 9 May 2006.

293 See, eg, J Gaudin, 'The OECD Privacy Principles—Can They Survive Technological Change? Part I' (1996) 3 *Privacy Law & Policy Reporter* 143, 144.

294 R Clarke, *Submission to the Senate Legal and Constitutional References Committee Inquiry into the Privacy Act 1988*, 25 February 2005, 2.

(a) should there be any additional limits on the collection of personal information;

(b) should agencies or organisations be required to obtain consent before using certain technologies to collect personal information? If so, should it be possible to refuse consent without any adverse consequences;

(c) should biometric information be included in the definition of 'sensitive information'; and

(d) should agencies or organisations be required to advise individuals of any misuse, loss or unauthorised access, modification or disclosure of personal information?

Question 11–4 Should the *Privacy Act* be technologically neutral?

Question 11–5 What issues are raised by the publication in electronic form of publicly available records such as public records, court records and media reports? Does the *Privacy Act* need to be amended in response to these issues?

12. Unique Multi-Purpose Identifiers

Contents

Introduction

12.1 In today's society 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 when individuals engage 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.

12.2 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]

12.3 A number of objects that are given to individuals by organisations contain unique identifiers. These are usually numbers—for example, a driver's license contains a number that is assigned to an individual for use by the relevant state or territory transport authority. 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 driver's licence or passport.[2] However, unique identifiers may also consist of biometric information, such as a fingerprint or information derived from an iris scan.

12.4 This chapter discusses unique identifiers assigned to individuals by governments for use by multiple government agencies and organisations (unique multi-purpose identifiers). The chapter commences by providing an overview of concerns that have been expressed about the impact on privacy of unique multi-purpose identifiers. It then examines the history of identification schemes in Australia before discussing the Australian Government's proposed Access Card. Finally, it considers identification schemes using unique multi-purpose identifiers in other countries. The collection, use and disclosure of single purpose identifiers is discussed in Chapter 4.[3]

Unique multi-purpose identifiers and privacy

12.5 Schemes involving unique multi-purpose identifiers can have a number of benefits. For example, they can increase administrative efficiency and enhance data accuracy.[4] However, they 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.[5] In liberal democratic societies governments are accountable to their citizens. It is argued that the introduction of a unique multi-purpose identifier symbolically reverses this tradition, making citizens accountable to their governments.[6] This could then open the way for 'further extensions of government power and … further restrictions on the individual's sphere of independent action'.[7]

---

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* (2004), [6.1].

3 The expression 'single purpose identifier' is used to describe an identifier allocated to an individual by an agency or organisation for use only by that agency or organisation.

4 See, eg, Council of Europe, *The Introduction and Use of Personal Identification Numbers: The Data Protection Issues* (1991).

5 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [3.7].

6 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.

7 Ibid, 163.

12.6 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.[8] 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.[9] Aliases may be used by a variety of people, such as artists and intelligence operatives.[10]

12.7 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. This could include 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 in order to market more effectively goods or services to him or her.

12.8 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'. The use of a unique multi-purpose identifier facilitates greatly the data-matching process. It is argued that one of the purposes of data-matching is to acquire evidence of wrongdoing before there is any suspicion that any wrongdoing has occurred. Accordingly, data-matching is said to amount to a 'warrantless search' that reverses the onus of proof required for traditional investigations into criminal behaviour.[11] In 2004, the former federal Privacy Commissioner, Malcolm Crompton, commented that:

> Given the strong drivers behind gathering more and more knowledge of individuals—defence against terrorism; combating fraud; solving and preventing crime; protecting our borders; saving taxpayer's money; increasing sales and turnover; not to mention the potential for individuals to live more conveniently in various ways—there is very strong pressure for data that can be linked, to be linked.[12]

12.9 The ability of a government to compile dossiers of personal information about individuals could have a 'chilling effect' on the activities of the government's citizens, who no longer have a private sphere in which to relax, experiment or engage in creative pursuits.[13]

---

8 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [3.37].

9 Ibid, Addendum, [22].

10 R Clarke, 'Just Another Piece of Plastic for your Wallet: The "Australia Card" Scheme' (1987) 5 *Prometheus* 1, 40.

11 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [50].

12 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 15.

13 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.

12.10 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.[14] 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.

12.11 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.

12.12 Finally, it has been argued that identity documents have had a long history of discriminatory uses for social control.[15] 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.[16]

12.13 The Council of Europe has stated that policy makers should evaluate carefully the costs and benefits of any scheme involving the use of unique identifiers. In the case of existing schemes using unique identifiers, it has recommended that restrictions be placed on the use of the identifiers to ensure that the scheme achieves 'the requisite balance between privacy and administrative efficiency'. This could be achieved, for example, by amending data protection legislation to ensure that it deals expressly with the use of identifiers by public powers. It also recommended that new schemes involving unique identifiers be introduced by legislation, and that the legislative framework clearly delineate the acceptable use of the identifiers. Further, it has recommended that specific controls and safeguards be introduced to govern data-matching by means of unique identifiers.[17]

---

14 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 14.

15 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 18 August 2006.

16 R Sobel, 'The Demeaning of Identity and Personhood in National Identification Systems' (2002) 15 *The Harvard Journal of Law and Technology* 319, 343–349.

17 Council of Europe, *The Introduction and Use of Personal Identification Numbers: The Data Protection Issues* (1991).

History of identification schemes in Australia

Identification schemes in wartime

12.14 Several identification schemes have been implemented in wartime Australia. During World War I, all aliens (non-British subjects) were required to register with local government officials.[18] After registration, they were required to notify officials if they changed their address[19] and to produce their certificates of registration on demand.[20]

12.15 During World War II, all aliens were again required to register with local government officials, after which they were issued with a certificate of registration.[21] Again, they were subject to continuing obligations to notify officials of any change of name or change of address.[22] 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.[23] They were then required to produce their identity cards if requested to do so by specified people, such as constables on duty.[24]

The Australia Card

12.16 In September 1985, the Australian Government announced its intention to develop a national identification scheme—the 'Australia Card' scheme[25]—to combat tax fraud, social security fraud and illegal immigration.[26] In November 1985, a Joint Select Committee on an Australia Card (the Committee) was appointed to inquire into the scheme. In May 1986, the Committee released its report. A majority of members opposed the introduction of the Australia Card scheme,[27] concluding that:

> the creation of a new bureaucracy of 2000 public servants within the [Health Insurance Commission], with the sole task of identifying every man, woman and child in Australia, is a wasteful exercise which will not address the problems of tax evasion and social security fraud but will provide the mechanism by which the very fabric of

---

18 *War Precautions (Alien Registration) Regulations 1916* (Cth) reg 5.
19 Ibid reg 9.
20 Ibid reg 12.
21 *Aliens Registration Act 1939* (Cth) ss 8, 13(1).
22 Ibid ss 9–12.
23 *National Security (Man Power) Regulations 1942* (Cth) reg 32.
24 Ibid regs 45, 45A.
25 P Keating (Treasurer), *Reform of the Australian Taxation System: Statement by the Treasurer The Hon Paul Keating*, 1 September 1985, 28–31.
26 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].
27 L Jordan, *E-brief: Identity Cards* (2006) Parliament of Australia—Parliamentary Library <www.aph.gov.au> at 21 April 2006.

> our society will be irreversibly altered, opening the way for the greatest attack on the privacy of individuals as the 'Identity Bureau' identifies, monitors, and updates information on every person in Australia.[28]

12.17 The report recommended a number of alternative reforms to address the issues of tax evasion, social security fraud and illegal immigration, such as the computerisation of all state and territory registries of births, deaths and marriages[29] and the introduction of an upgraded, high integrity tax file number scheme.[30]

12.18 The Australian Government did not formally respond to the Committee's report.[31] However, in October 1986 the Australia Card Bill 1986 (Cth) was introduced into Parliament. During the Bill's second reading speech the Minister for Health, the Hon Neal Blewett MP, rejected the Committee's recommendations regarding the enhanced tax file number scheme, describing them as a 'soft and fuzzy alternative to the Australia Card'.[32]

12.19 The identification scheme set out in the Australia Card Bill was as follows. All Australian citizens (and certain non-citizens) were entitled to apply to the Health Insurance Commission (HIC) for an Australia Card.[33] Cards for adult citizens would contain: the card's expiry date; information about the number of times the card had been issued or renewed; the cardholder's name, photograph, and signature; and a unique identification number.[34] Cards for certain non-citizens could also display information about the cardholder's eligibility to receive Medicare benefits or obtain employment.[35]

12.20 Australia Cards would be valid for between three and seven years, or five and six years, depending on when they were issued.[36] Individuals would be required to produce their Australia Card in a number of circumstances, such as when transacting with financial institutions,[37] buying shares,[38] commencing employment,[39] or claiming

---

28 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [4.55].
29 Ibid, Rec 2(a).
30 Ibid, Rec 12(a)–(d).
31 L Jordan, *E-brief: Identity Cards* (2006) Parliament of Australia—Parliamentary Library <www.aph.gov.au> at 21 April 2006.
32 Commonwealth, *Parliamentary Debates*, House of Representatives, 22 October 1986, 161 (N Blewett—Minister for Health).
33 Australia Card Bill 1986 (Cth) cls 10, 11.
34 Ibid cl 17(3), (5), (7).
35 Ibid cl 17(4).
36 Ibid cl 18.
37 Ibid cl 40.
38 Ibid cl 47.
39 Ibid cl 49.

Medicare or social security benefits.[40] It was not mandatory to carry the card,[41] although individuals were entitled to use the card as a form of identification.[42]

12.21 The Bill also provided for the establishment of an Australia Card Register, to be maintained by the HIC. The Register would contain information such as the name, date of birth, sex, address, and citizenship status of the cardholder.[43] Three government agencies were entitled to access the Register—the Australian Taxation Office, the Department of Social Security and the HIC[44]—and a record would be made of every access or attempted access to the Register.[45]

12.22 On two occasions the Australia Card Bill was passed by the House of Representatives[46] only to be rejected by the Senate.[47] 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.[48]

12.23 Little mention was made of the Australia Card during the ensuing federal election campaign.[49] 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. From mid-1985 to June 1987, public opinion polls indicated that 68% of Australians supported the Australia Card scheme.[50] However, in what has been described as 'one of the most massive shifts in public opinion' in Australian politics, public support for the scheme had fallen to 39% by September 1987.[51] The Bill was ultimately laid aside after members of the Opposition indicated that they would disallow regulations that were required to bring crucial clauses of the Bill into effect.[52]

The enhanced Tax File Number scheme

12.24 Before 1988, tax file numbers (TFNs) were simply numbers used by the Australian Taxation Office (ATO) to match taxpayers' returns to the ATO's computer

40 Ibid cls 52, 54.
41 Ibid cl 8.
42 Ibid cl 8(3).
43 Ibid cl 25, sch 1.
44 Ibid cls 60–62.
45 Ibid cl 25(3).
46 On 14 November 1986 and 25 March 1987: See L Jordan, *E-brief: Identity Cards* (2006) Parliament of Australia—Parliamentary Library <www.aph.gov.au> at 21 April 2006.
47 On 10 December 1986 and 2 April 1987: See Ibid.
48 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.
49 R Clarke, 'The Australia Card: Postscript' (1988) 18 *Computers & Society* 10, 10.
50 G Greenleaf, 'Lessons from the Australia Card—Deux ex Machina?' (1988) 3(6) *Computer Law and Security Report* 6, 6.
51 Ibid, 7.
52 Ibid, 6.

records.[53] 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.[54]

12.25 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.[55] He stated that the scheme would not be a national identification scheme and that the tax office would be the only government agency to use TFNs to identify and register its client base.[56] In 1988, legislation establishing a new TFN scheme was passed.[57]

12.26 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.[58] Under the scheme, which still operates today, any person can apply to the Commissioner of Taxation for a TFN.[59] If satisfied of an applicant's identity, the Commissioner will provide the applicant with a unique TFN,[60] which can then be quoted when the applicant commences employment or engages in certain investment activities.

12.27 At the time the TFN scheme was introduced there were concerns that it would become a 'de facto national identification scheme'[61] 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 any TFN (including the TFN of entities other than natural persons) in unauthorised circumstances.[62] 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.

12.28 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'.[63] 'Tax file number information' is defined as 'information …

---

53 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), [4.8].

54 Ibid, [4.8].

55 P Keating (Treasurer), *Reform of the Australian Taxation System: Statement by the Treasurer The Hon Paul Keating*, 1 September 1985.

56 Ibid.

57 *Taxation Laws Amendment (Tax File Numbers) Act 1988* (Cth).

58 Commonwealth, *Parliamentary Debates*, House of Representatives, 1 September 1988, 858 (P Keating—Treasurer).

59 *Income Tax Assessment Act 1936* (Cth) s 202B.

60 Ibid s 202BA.

61 Parliament of Australia—Senate Standing Committee on Legal and Constitutional Affairs, *Feasibility of a National ID Scheme; The Tax File Number* (1988), Ch 10.

62 *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.

63 Interim guidelines set out in sch 2 of the *Privacy Act 1988* (Cth) applied until the Privacy Commissioner's guidelines issued under s 17 took effect: *Privacy Act 1988* (Cth) s 17(4).

that records the tax file number of a person in a manner connecting it with the person's identity'.[64] The Privacy Commissioner's guidelines are binding on all 'file number recipients'[65]—namely, people who are 'in possession or control of a record that contains tax file number information'.[66]

12.29 The Privacy Commissioner issued TFN guidelines in 1992.[67] These Guidelines provide that the TFN scheme is not to be used as a national identification scheme.[68] 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.[69] TFNs can only be collected by certain persons and organisations[70] 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.[71] 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.[72]

12.30 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.[73] Further, file number recipients may dispose of TFN information if it is no longer required for legal or administrative purposes.[74]

12.31 In 2004–05, complaints concerning TFNs accounted for less than 5% of the complaints received by the Privacy Commissioner.[75] Other functions of the Privacy Commissioner relating to TFNs, such as the power of the Privacy Commissioner to investigate acts or practices that may be in breach of the guidelines, are discussed in Chapter 6.

---

64 *Privacy Act 1988* (Cth) s 6.
65 Ibid s 18.
66 Ibid s 11.
67 Office of the Federal Privacy Commissioner, *Tax File Number Guidelines* (1992).
68 Ibid, 1.1.
69 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 12.
70 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).
71 Ibid, [2.1], [5.1].
72 Ibid, [2.3].
73 Ibid, [6.1].
74 Ibid, [6.2].
75 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2004–30 June 2005* (2005), 40.

12.32 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.[76] Further, since 1991 the Department of Social Security (now Centrelink) has been permitted to use TFNs to match records between the ATO and specified assistance agencies,[77] such as Centrelink and the Department of Veterans' Affairs,[78] in order to 'detect where a person has provided inconsistent information to one or more agencies and is thereby receiving incorrect payments'.[79]

12.33 The Privacy Commissioner has issued legally binding guidelines relating to this data-matching program which contain safeguards for individuals affected by it. For example, the guidelines require individuals to be informed before information supplied by them is used in the data-matching program, or as soon as practicable after it has been so used.[80] The guidelines also prevent agencies from linking or merging information used in the data-matching program in order to create a new separate register of information about individuals.[81]

12.34 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.[82] 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'.[83]

12.35 The schemes that regulate the use of TFNs may impose a regulatory burden on businesses. For example, the Privacy Commissioner's TFN guidelines prevent organisations from recording a TFN provided for a purpose not connected with the operation of a taxation, assistance agency or superannuation law. In its submission to the 2005 Taskforce on Reducing the Regulatory Burden on Business, the Mortgage Industry Association of Australia noted that individuals often provide documents containing TFNs to mortgage industry participants and that removing the TFN from these documents was time-consuming.[84] One stakeholder has submitted that limitations

---

76 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.

77 *Data-matching Program (Assistance and Tax) Act 1990* (Cth).

78 Ibid s 3.

79 Commonwealth, *Parliamentary Debates*, House of Representatives, 20 December 1990, 4871 (G Bilney—Minister for Defence Science and Personnel).

80 Office of the Federal Privacy Commissioner, *Schedule—Data-matching Program (Assistance and Tax) Guidelines* (1997), [5.4].

81 Ibid, [7.1].

82 Office of the Privacy Commissioner, *An Introductory Guide to Privacy Impact Assessment for Australian Government and ACT Government Agencies*, Consultation Draft (2004), [3].

83 M Crompton, 'Proof of ID Required? Getting Identity Management Right' (Paper presented at Australian IT Security Forum, 30 March 2004), 13.

84 Mortgage Industry Association of Australia, *Submission to the Taskforce on Reducing the Regulatory Burden on Business*, 1 March 2005.

on the disclosure of TFNs means that it is necessary to contact shareholders every time a company's shareholder register merges with another company's register or splits into different registers.[85]

Question 12–1 Are the schemes that regulate Tax File Numbers appropriate and effective?

The Medicare smart card

12.36 Medicare (formerly known as Medibank) commenced in 1975 to enable all eligible Australian residents to access affordable health care.[86] 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.[87]

12.37 Federal legislation contains secrecy provisions that prevent officers exercising powers under certain Acts from disclosing personal information acquired during the course of their employment.[88] In addition, legislation prohibits the disclosure of Medicare numbers provided for the purpose of participation in the pharmaceutical benefits scheme.[89] Further, the Privacy Commissioner has issued guidelines that regulate the handling of information obtained by an agency in connection with a claim for payment of a benefit under the Medicare Benefits Program or the Pharmaceutical Benefits Program.[90]

12.38 On 24 June 2004, the Minister for Health and Ageing, the Hon Tony Abbott MP, announced the introduction of a new Medicare smart card.[91] 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.[92] It was predicted that the card could later store patient information to facilitate

85 Link Market Service, *Submission PR 2,* 24 February 2006.
86 *Health Insurance Act 1973* (Cth).
87 Medicare Australia, *About Medicare Australia* <www.medicareaustralia.gov.au> at 21 August 2006. The Access Card is discussed further below.
88 See *National Health Act 1953* (Cth) ss 135A, 135AA; *Health Insurance Act 1973* (Cth) s 130.
89 *National Health Act 1953* (Cth) s 135AAA.
90 Office of the Federal Privacy Commissioner, *Medicare and Pharmaceutical Benefits Programs Privacy Guidelines: Issued under Section 135AA of the National Health Act 1953* (1997).
91 T Abbott (Minister for Health and Ageing), 'New Medicare Smartcards' (Press Release, 24 June 2004). Smart card technology is discussed in Ch 11.
92 Medicare Australia, *Medicare Smartcard: Frequently Asked Questions* (2005) <www.medicareaustralia.gov.au/resources/medicare_smartcard/ma_0993_medicare_smartcard_faq_250805.pdf> at 12 September 2006.

patient identification in an emergency.[93] It could also later facilitate access to an electronic system of health information called Health*Connect.*[94] 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.[95]

12.39 The Medicare smart card was to be introduced on an 'opt-in' basis in Tasmania before being rolled out nationally.[96] However, there was limited take-up of the scheme, and it was terminated on 25 May 2006 in light of the Australian Government's decision to introduce the Access Card.[97]

Other proposed identification schemes

12.40 After the bombings in London in July 2005, the Prime Minister, the Hon John Howard MP, stated that the introduction of a national identification scheme was an issue that should be 'back on the table'.[98] The introduction of such a scheme was discussed on a number of occasions during 2005 and early 2006.[99] However, on 26 April 2006 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 services (the Access Card).[100]

The proposed Health and Social Services Access Card

Overview of the Access Card scheme

12.41 The Access Card scheme will enable consumers to access all health and social services with one card; inform only one agency of changed personal information; access emergency relief payments through automatic teller machines and through Electronic Funds Transfer at Point of Sale (EFTPOS);[101] and store information on the

93 Ibid.
94 Ibid. Health*Connect* is discussed further in Ch 8.
95 R LeMay, 'Hackers on Medicare Smart Card Waiting List', *ZDNet Australia* (online), 24 February 2005, <www.zdnet.com.au/news/>.
96 T Abbott (Minister for Health and Ageing), 'New Medicare Smartcards' (Press Release, 24 June 2004).
97 Commonwealth, *Parliamentary Debates*, Senate Finance and Public Administration Legislation Committee, 25 May 2006, 126.
98 J Howard (Prime Minister), *Doorstop Interview*, 15 July 2005.
99 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.
100 J Howard (Prime Minister), P Ruddock (Attorney-General) and J Hockey (Minister for Human Services), *Joint Press Conference*, 26 April 2006.
101 'Smart Card Could Access Govt Payments Through ATMs: Hockey', *ABC News Online*, 28 June 2006, <www.abc.net.au/news>.

card which may be useful in an emergency.[102] It also aims to reduce fraud on health and social services, and financial losses caused by administrative error.

12.42 The Access Card will replace 17 existing health care and social services cards and vouchers.[103] It will display the cardholder's name and photograph on its front, and the cardholder's signature and card number on its back.[104] The card number will be the cardholder's current Medicare number, reformatted with extra digits where necessary to ensure it is unique.[105] Other personal information, such as the cardholder's photograph, address, date of birth, concession status, and details of the cardholder's children or dependants will be stored on a microchip embedded in the card.[106] The cardholder may also choose to store further information on the card's chip, such as 'emergency contact details, allergies, health alerts, chronic illnesses, immunisation information or organ donor status'.[107]

12.43 Registration for the card is scheduled to commence in 2008 and conclude in early 2010, after which a card will be required in order to access any health or social services.[108] To register for an Access Card, each individual will be required to present substantial evidence of his or her identity. This evidence will be scanned and stored, along with the information on the card and the chip, on a database called the Secure Customer Registration Service (SCRS).[109] The Australian Government has stated that the SCRS will be maintained separately from existing agency databases.[110]

12.44 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

---

102 Office of Access Card, *Fact Sheet—Supporting Information* (2006) Australian Government Department of Human Services, <www.humanservices.gov.au/access/fact_sheets/supporting_info.htm> at 19 June 2006.

103 The Medicare card, Medicare Australia Organ Donor Registration card, Medicare Reciprocal Health Care Agreement card, PBS Safety Net Entitlement card, PBS Concession card, Cleft Lip and Palate card, Centrelink Pensioner Concession card, Centrelink Healthcare card, Centrelink Foster Child Care card, Centrelink Low Income Healthcare card, Centrelink Commonwealth Seniors card, Centrelink Electronic Benefit Transfer, DVA Gold Repatriation Health card, DVA White Repatriation Health card, DVA Repatriation Pharmaceutical Benefits card, War Widow/Widow's Transport Concession card and the Office of Hearing Services voucher: see Ibid.

104 Office of Access Card, *Fact Sheet—Technology* (2006) Australian Government Department of Human Services, <www.humanservices.gov.au/access/fact_sheets/technology.htm> at 16 June 2006.

105 KPMG, *Health and Social Services Smart Card Initiative—Volume 1: Business Case Public Extract* (2006) Prepared for the Department of Human Services, [6.1.6].

106 Office of Access Card, *Fact Sheet—Technology* (2006) Australian Government Department of Human Services, <www.humanservices.gov.au/access/fact_sheets/technology.htm> at 16 June 2006.

107 Ibid.

108 J Howard (Prime Minister), 'Government to Proceed with Access Card' (Press Release, 26 April 2006).

109 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 1: The Australian Government Health and Social Services Access Card* (2006), 12.

110 Ibid, 12.

and $3 billion dollars over 10 years.[111] The scheme will be administered by the Office of Access Card within the Australian Government Department of Human Services.[112]

The Access Card Consumer and Privacy Taskforce

12.45 On 24 May 2006, the Minister for Human Services, the Hon Joe Hockey MP, announced the establishment of the Access Card Consumer and Privacy Taskforce (the Taskforce). The Taskforce will provide 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.[113]

12.46 On 15 June 2006, the Taskforce released a Discussion Paper on consumer and privacy aspects of the scheme.[114] As at 3 August 2006, the Taskforce had received over 70 submissions in response to its Discussion Paper and had met with approximately 50 consumer and privacy organisations.[115] The Taskforce intends to report to the Australian Government about certain aspects of the scheme in October 2006.[116]

The *Privacy Act* and the Access Card scheme

12.47 As discussed in Chapter 4, the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) in the *Privacy Act* set out minimum legal standards to be observed by agencies and organisations that deal with personal information. The IPPs do not deal explicitly with identifiers. However, the NPPs prevent organisations from adopting identifiers assigned to individuals by agencies unless they have been authorised to do so by regulation.[117] The NPPs also limit the circumstances in which organisations can use or disclose identifiers assigned to individuals by agencies.[118] The purpose of the principle limiting the use and disclosure of identifiers was to 'prevent the gradual adoption of government identity numbers as de facto universal identity numbers'.[119]

12.48 It is assumed that the *Privacy Act* will govern the handling of personal information collected for the Access Card scheme. However, the extent to which it will do so is uncertain due to the lack of publicly available information about the structure and operation of the scheme.

---

111 KPMG, *Health and Social Services Smart Card Initiative—Volume 1: Business Case Public Extract* (2006) Prepared for the Department of Human Services, [3.5].

112 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 1: The Australian Government Health and Social Services Access Card* (2006).

113 Ibid, 4.

114 Ibid.

115 Access Card Consumer and Privacy Taskforce, 'Quality Submissions to Guide Development of Access Card' (Press Release, 3 August 2006).

116 Access Card Consumer and Privacy Taskforce, *Discussion Paper Number 1: The Australian Government Health and Social Services Access Card* (2006), 5.

117 *Privacy Act 1988* (Cth) sch 3, NPP 7.1, 7.1A.

118 Ibid sch 3, NPP 7.2.

119 Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth).

12.49 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.[120] Another is that information in the SCRS will be targeted by those wishing to acquire large amounts of personal information for some kind of gain,[121] or accessed for illegitimate purposes by government employees.[122] 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.[123] Some have argued that the Access Card scheme is the same as the failed Australia Card scheme.[124]

12.50 Concern has also been expressed about function creep in the context of the Access Card scheme.[125] Currently, the *Privacy Act* allows the use or disclosure of personal information if it is required or authorised by law.[126] 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.[127] 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.[128]

12.51 It is difficult to assess concerns about the impact of the Access Card scheme on privacy until the architecture of the card is finalised and made public. 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 next report of the Taskforce.

Identification schemes in other countries

12.52 This section discusses overseas experiences with multi-purpose identification schemes. It focuses primarily on countries with similar legal systems to Australia—that

---

120 See, eg, Australian Privacy Foundation, *Why Every Australian Should Oppose the 'Access Card': The Arguments Against a National ID Card System* (2006).

121 See, eg, Ibid.

122 'Centrelink Scandal Highlights Smartcard Fears', *The Epoch Times* (online), 25 August 2006, <www.theepochtimes.com>.

123 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.

124 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.

125 See, eg, M Franklin, 'MP Warns of Access Card Misuse', *The Courier-Mail* (Brisbane), 18 July 2006, 4.

126 *Privacy Act 1988* (Cth) s 14, IPPs 10, 11; sch 3, NPP 2.

127 A Stafford, 'Access Card Could Link to Surveillance', *The Age* (Melbourne), 5 June 2006, 9.

128 *Privacy Act 1988* (Cth) s 14, IPP 10; sch 3, NPP 2.

is, developed Western countries with a common law tradition. However, it will also discuss identification schemes in the European Union and other select countries.

Canada

12.53 In the 1990s the Canadian Government rejected a proposal to replace the Social Insurance Number with a national identity card, concluding that the introduction of a national identification scheme would be expensive and detrimental to privacy.[129] In 2002, the Minister for Citizenship and Immigration, the Hon Denis Coderre, called for another debate on the issue of a national identification scheme.[130] In October 2003, an interim report of the House of Commons Standing Committee on Citizenship and Immigration set out a number of community concerns about the scheme.[131] Many of these related to the impact of such a scheme on privacy. For example, some argue that a national identification scheme could violate the *Canadian Charter of Rights and Freedoms*. The issue was not resolved at the time of the 2004 federal election and has not been raised since.[132]

The United States

12.54 There is no national identification scheme in the United States. Since the 1970s, proposals to change a widely used identifier, the Social Security Number, into a unique multi-purpose national identifier have been rejected on a number of occasions.[133] However, it has been argued that the *REAL ID Act of 2005*,[134] which prohibits federal agencies from accepting state-issued driver's licences as evidence of identity unless the licences comply with certain standards, will turn driver's licences into unofficial national identification cards.[135]

The United Kingdom

12.55 National identification schemes were operational in the United Kingdom during World War I and World War II.[136] The scheme introduced in World War I was withdrawn at the end of the war.[137] The scheme introduced in 1939, however, continued to operate after the war. It was withdrawn in 1952 after the King's Bench

---

129 Parliament of Canada—House of Commons Standing Committee on Citizenship and Immigration, *A National Identity Card for Canada?* (2003), 4.

130 'National ID Cards', *CBC News Online* (online), 7 December 2004, <www.cbc.ca/news/>.

131 Parliament of Canada—House of Commons Standing Committee on Citizenship and Immigration, *A National Identity Card for Canada?* (2003), 9–14.

132 L Jordan, *E-brief: Identity Cards* (2006) Parliament of Australia—Parliamentary Library <www.aph.gov.au> at 21 April 2006.

133 Electronic Privacy Information Centre, *National ID Cards and the REAL ID Act* <www.epic.org/privacy/id_cards> at 16 August 2006.

134 *REAL ID Act of 2005* Pub L 109–13 (US).

135 Electronic Privacy Information Centre, *National ID Cards and the REAL ID Act* <www.epic.org/privacy/id_cards> at 16 August 2006.

136 *National Registration Act 1915* (UK); *National Registration Act 1939* (UK).

137 United Kingdom Parliament—House of Commons Library, *The Identity Cards Bill: Bill 9 of 2005–06* (2005), 7.

Division of the High Court expressed disapproval of the routine use of identity cards by authorities in peacetime.[138]

12.56 Between 1952 and 2004 there were several unsuccessful attempts to introduce a national identification system in the United Kingdom.[139] For example, a proposal to introduce a Unique Personal Identifier was considered and rejected by the Committee on Data Protection in 1978,[140] and a proposal to introduce a national identification scheme raised by the Prime Minister, the Rt Hon John Major MP, in 1995 was not pursued after 1997.[141]

12.57 In 2001, after the terrorist attacks on the United States, the issue of a national identification scheme was raised again.[142] In July 2002, a consultation paper on 'entitlement cards' was released[143] and in November 2003 the Secretary of State for the Home Department, the Rt Hon David Plunkett MP, announced that a national identification scheme would be introduced in the United Kingdom.[144]

12.58 In April 2005, a Bill to introduce a national identification scheme lapsed with the dissolution of Parliament.[145] In May 2005, a second, similar Bill was introduced into Parliament. It was passed and received Royal Assent on 30 March 2006.[146] The *Identity Cards Act 2006* (UK) requires every individual applying for a 'designated document', such as a passport, to apply to have certain information—including his or her name, address, gender, date of birth, fingerprints, iris scan and facial image—included in a National Identification Register.[147] Upon registration, each individual will be issued with a unique registration number that will be included on his or her identity card.[148] The scheme is expected to commence in 2008–09[149] and until 2010 individuals

---

138 *Willcock v Muckle* (1957) 49 LGR 584, 587; Privacy International, *History of ID Cards in the United Kingdom* (1997) <www.privacyinternational.org> at 17 August 2006.

139 Privacy International, *History of ID Cards in the United Kingdom* (1997) <www.privacyinternational.org> at 17 August 2006.

140 Parliament of Australia—Joint Select Committee on an Australia Card, *Report of the Joint Select Committee on an Australia Card* (1986), Addendum, [76].

141 United Kingdom Parliament—House of Commons Library, *The Identity Cards Bill: Bill 9 of 2005–06* (2005), 8.

142 Privacy International, *Background on the UK Entitlement Card* (2003) <www.privacyinternational.org> at 18 August 2006; United Kingdom Parliament—House of Commons Library, *The Identity Cards Bill: Bill 9 of 2005–06* (2005), 9.

143 United Kingdom Government Home Office, *Entitlement Cards and Identity Fraud: A Consultation Paper* (2002).

144 D Blunkett (Home Secretary), 'David Blunkett: National ID Scheme to be Introduced' (Press Release, 11 November 2003).

145 Identity Cards Bill 2004–05 (UK).

146 *Identity Cards Act 2006* (UK).

147 Ibid ss 1–3, 4.

148 Ibid ss 4–7.

149 United Kingdom Government Home Office Identity and Passport Service, *How to Get Your ID Card and How it Will be Produced* <www.identitycards.gov.uk/scheme.asp> at 18 August 2006.

will be given the choice about whether they wish to be issued with an identity card after registration.[150]

Other European Union countries

12.59 Most European Union countries have national identification schemes.[151] It is compulsory to carry identification cards in some countries, such as Belgium, Germany and Spain, and voluntary in most others.[152] It has been argued that citizens of civil law countries have different attitudes towards identification schemes than those of common law countries because they have different views about the relationship of the individual to the state.[153]

Other countries

12.60 National identification cards have been in use in Malaysia since 1949.[154] However, in 2001 the Malaysian Government introduced a multi-purpose smart identification card called 'MyKad'.[155] The card contains substantial amounts of personal information about the cardholder. For example, the card's chip contains information about the cardholder's race, religion (if the cardholder is Muslim) and health, as well as containing an image of the cardholder's thumbprint.[156] The card can also be used for a variety of other functions. For example, it includes an 'electronic purse' that enables it to be used to purchase goods or services[157] and it can also be used to carry out banking activities at ATMs.[158]

12.61 A national identification scheme was introduced in Hong Kong at the end of World War II.[159] Every person in Hong Kong is required to register and receive an identification card, unless exempted by regulations.[160] After registration, every person is required to provide his or her identity card in all dealings with government officials.[161] Since 2003, existing identification cards are being replaced with multi-purpose smart identification cards. Currently, additional uses of identity cards are

150 Ibid.
151 See United Kingdom Parliament—House of Commons Library, *The Identity Cards Bill: Bill 9 of 2005–06* (2005), 11.
152 Ibid, 11.
153 Parliament of Canada—House of Commons Standing Committee on Citizenship and Immigration, *A National Identity Card for Canada?* (2003).
154 M Thomas, 'Is Malaysia's MyKad the "One Card to Rule Them All"? The Urgent Need to Develop a Proper Legal Framework for the Protection of Personal Information in Malaysia' (2004) 28 *Melbourne University Law Review* 474, 475.
155 Ibid, 475.
156 Ibid, 481.
157 Ibid, 481.
158 Ibid, 482.
159 G Greenleaf, *Hong Kong's ID Card—An Overview* (2006) University of New South Wales <www2.austlii.edu.au/privacy/HKID/HKID_outline.html> at 16 August 2006.
160 *Registration of Persons Ordinance* Cap 177 (HK) s 3.
161 Ibid s 5(1)(b).

limited to use as a library card, a driver's licence, and for the purpose of engaging in online transactions.[162]

Question 12–2 What unique multi-purpose identifiers are currently in use in Australia? What are the benefits and privacy concerns of using unique multi-purpose identifiers in transactions with agencies or organisations?

Question 12–3 What role, if any, should the *Privacy Act* play in the regulation of unique multi-purpose identifiers?

162 Government of the Hong Kong Special Administrative Region of the People's Republic of China, *Applications on Smart ID Card* (2006) <www.smartid.gov.hk/t_en/app/index.html> at 16 August 2006.

13. Transborder Data Protection

Contents

Transborder data flow

13.1 Transborder data flow refers to the movement of personal 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 there should be a harmonisation of efforts to protect personal information.[2]

> 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]

13.2 The appropriate protection of transborder data flow is an issue for individuals, businesses and government. Overseas business processing centres are increasingly handling customer data in such sensitive areas as processing credit card applications

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.
3 K Sainty and A Ailwood, *Managing Compliance in the Global Space—Transborder Data Flow* (2004) Allens Arthur Robinson, 1.

and bills, mortgage applications, insurance claims and help desk services.[4] It is important for Australians to feel confident that if an Australian organisation transfers their personal information outside Australia, it will be protected to the same standard that they would enjoy here.

13.3 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. The 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.[5] 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.[6]

13.4 More recent examples of these instruments are the privacy principles adopted by the European Union under the 1995 European Union Directive[7] (EU Directive) and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[8] The Asia-Pacific Privacy Charter Council (the APPC Council), a regional non-government expert group, has also done work on developing independent privacy standards for privacy protection in the Asia-Pacific region.[9] Australia's ability to meet the expectations of privacy protection demanded by the international community is important to ensure that businesses are not disadvantaged in an international market.

13.5 This chapter first will look 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 information to countries with differing privacy regimes. It considers the adequacy of the protection offered under NPP 9, and the difficulties that may be experienced by businesses in complying with its requirements.

---

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 Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), Guideline 18. The OECD Guidelines are discussed in greater detail in Ch 4.

6 The IPPs and OECD Guidelines do not contain a comparable transborder data principle to that in NPP 9. This issue is discussed in Ch 4.

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).

8 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005).

9 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 11 September 2006. These instruments are discussed later in the chapter.

13.6 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. Finally the chapter considers other international models of transborder data transfer protection.

Privacy Act 1988 (Cth)

Extra-territorial operation of the *Privacy Act*

13.7 Section 5B of the *Privacy Act* may be summarised as follows. It 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

- the organisation 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.

13.8 Section 5B(4) extends the enforcement powers of the Privacy Commissioner to overseas complaints that fall within the criteria in s 5B(1).[10]

13.9 The purpose of 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.[11] However, the privacy laws of another country 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.*[12]

National Privacy Principle 9

13.10 National Privacy Principle 9 dictates the circumstances in which an organisation can transfer the personal information it holds in Australia to someone in a foreign country.[13] As with the other private sector provisions, it was introduced in 2000 as part of the extension of privacy principles to the private sector. NPP 9 was intended to meet international concerns and changing obligations.[14]

---

10 The enforcement powers of the Privacy Commissioner are considered in detail in Ch 6.
11 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [1-460].
12 *Privacy Act 1988* (Cth) s 13D.
13 NPP 9 is also discussed in Ch 4.
14 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.

13.11 NPP 9 prohibits the transfer by an organisation of an individual's personal information to someone other than that individual or organisation unless a number of conditions are satisfied.[15] It states that:

> An organisation in Australia or an external Territory may transfer personal information about an individual to someone (other than the organisation or the individual) who is in a foreign country only if:
>
> (a) the 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 National Privacy Principles; or
>
> (b) the individual consents to the transfer; or
>
> (c) 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; or
>
> (d) 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; or
>
> (e) all of the following apply:
>
> (i) the transfer is for the benefit of the individual;
>
> (ii) it is impracticable to obtain the consent of the individual to that transfer;
>
> (iii) if it were practicable to obtain such consent, the individual would be likely to give it; or
>
> (f) the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

13.12 The principle is largely modelled on arts 25 and 26 of the EU Directive, which aims to ensure continued protection of personal information when data is sent from its originating country.[16] 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.[17]

13.13 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

---

15 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.

16 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. Article 25(1) is set out later in this chapter.

17 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.

that is not subject to privacy law, or a private sector organisation that is exempt from the federal *Privacy Act*.[18] Where the transfer of information overseas is to the same organisation, not a third party, NPP 9 does not apply. The general provisions of the *Privacy Act* are applied extra-territorially by virtue of s 5B.

13.14 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.[19] This amendment was made by excluding NPP 9 from the citizenship and residency requirements of s 5B(1).

13.15 The nationality and residency limitations on the Privacy Commissioner's power to investigate complaints relating to the correction of personal information were also removed at this time.[20] These changes were made to address the European Commission's concern that Australian law was not sufficiently compatible with the EU Directive. Under the previous provisions, EU citizens would not have been protected against their data being exported to Australian businesses in foreign countries that had inadequate privacy regimes.[21]

13.16 The major criticisms of NPP 9 relate to: the perceived weakness of the tests for a 'reasonable belief' (NPP 9(a)) and the taking of 'reasonable steps' (NPP 9(f)); 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.

Reasonably believes

13.17 NPP 9(a) states that an organisation may transfer 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.

13.18 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, for instance, provides that the country in question *must have* an adequate level of protection. Professor Graham Greenleaf notes 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.*[22]

---

18 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.

19 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [1-460].

20 *Privacy Amendment Act 2004* (Cth).

21 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), 3.

22 Ibid, 8.

13.19 The Office of the Privacy Commissioner (OPC) Guidelines to the National Privacy Principles 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.[23]

13.20 It is not clear what other action, if any, would be sufficient to satisfy the 'reasonable belief' requirement.

Substantially similar principles

13.21 The *Privacy Act* does not provide a definition of what constitutes a 'substantially similar' set of principles for the purposes of NPP 9(a).[24] In the Office of the Privacy Commissioner review of the private sector provisions of the *Privacy Act* (OPC Review), the OPC noted that stakeholders had expressed frustration at the lack of guidance regarding the countries whose laws provide adequate protection equivalent to the NPPs. Many stakeholders stated that they had neither the expertise nor the resources to assess a foreign country's privacy laws.[25] This issue is discussed further below, in the context of the role of the OPC.

Reasonable steps

13.22 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 National Privacy Principles. This exception has been criticised as 'weak and imprecise' because it does not allow an individual recourse where an organisation has not adequately fulfilled the 'reasonable steps' requirement.[26]

13.23 There is also a concern 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.[27] Once the organisation has transferred the

---

23 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].

24 J Douglas-Stewart, *Annotated National Privacy Principles* (2005), [2-5800].

25 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 77.

26 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.

27 As well as under the federal *Privacy Act,* 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).

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.

13.24 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.

Interaction with NPP 2

13.25 NPP 2, which regulates the use and disclosure of personal information, contains a note that states that an organisation is also subject to the requirements of NPP 9 if it transfers personal information to a *person* in a foreign country. Given that NPP 9 applies to the transfer of information to 'someone' other than the individual or the organisation itself, the question arises whether the scope of 'someone' should be clarified—for example, to make it clear whether it is intended to cover releases of personal information to organisations and government bodies as well as individuals.

13.26 The ALRC is interested in hearing whether the relationship between NPP 2 (as it deals with disclosure) and NPP 9 (as it deals with transfer) requires further clarification, especially given that NPP 9 states that a transfer of data overseas can occur *only* in specified circumstances.

Question 13–1 Does NPP 9 provide adequate and appropriate protection for personal information transferred from Australia to a foreign country? Does the relationship between NPP 2 (disclosure of personal information) and NPP 9 (international transfer of personal information) need to be clarified?

Related bodies corporate

13.27 Another issue arises regarding the interaction between the exemption for related companies under s 13B(1) and NPP 9. 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.[28] As noted above, the *Privacy Act* operates extra-territorially in these circumstances by virtue of s 5B.

13.28 However, a company transferring personal information overseas to another related company 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 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.[29]

13.29 In submissions to the OPC Review, a number of stakeholders called for clarification in the way that NPP 9 and s 13B(1) operate together. 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.[30]

13.30 In its final report, the OPC points out 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.

> 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*.[31]

13.31 The view of the OPC is that where information is transferred outside of Australia and the extraterritorial provisions do not apply, it is in the public interest that NPP 9 applies. The OPC therefore did not recommend excluding related corporations from having to comply with NPP 9.[32]

13.32 In its submission to the Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Senate Committee privacy inquiry), the Australian Privacy Foundation (APF) argued that s 13B was complex and difficult to understand

---

28 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 58.

29 This definition is from the *Corporations Act 2001* (Cth), s 50. For a general discussion of the exemption, see Ch 5.

30 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 77.

31 Ibid, 79.

32 Ibid, 79.

and 'too generous in allowing exchanges of information between related companies which effectively avoid some of the NPP obligations'.[33] 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.[34]

13.33 The APF argued that the exemption under s 13B should be removed and that related companies should be treated as third parties.[35]

Question 13–2 Should the *Privacy Act* be amended to clarify that NPP 9 applies when personal information is transferred outside Australia to a related body corporate?

The role of the Privacy Commissioner

13.34 As noted above, it was suggested during the OPC review that the OPC should provide greater guidance to businesses on how to comply with NPP 9, and on the adequacy or otherwise of privacy protections available in overseas jurisdictions.[36]

List of overseas jurisdictions

13.35 The OPC Review noted that:

> 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.[37]

13.36 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 safely transfer information. The OPC rejected this 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 the Office to undertake.[38]

---

33 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), [4.171].
34 Ibid, [4.171].
35 Ibid, [4.171].
36 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.
37 Ibid, 78.
38 Ibid, 79.

13.37 An alternative view is that, if assessment of a country's privacy compatibility is complex, then it is in the interests of ensuring the best possible advice that a central body of experts be tasked with assessing these regimes. As previously noted, the OPC has suggested that an organisation seek legal advice to ensure that they have evidence to meet the requirement of 'reasonable belief' or 'reasonable steps'.[39]

13.38 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'.[40]

> 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.[41]

Contractual arrangements

13.39 The final report of the OPC Review noted 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.[42]

13.40 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. However, some concerns were raised regarding the additional cost of this method of ensuring compliance.[43]

13.41 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.

---

39 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), 59.

40 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.

41 Ibid, 7.

42 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78 (internal footnotes omitted).

43 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.

> 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.[44]

13.42 However, rather than publishing standard contractual provisions, the OPC instead recommended that the OPC should itself 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.[45]

13.43 The ALRC is interested in views as to the appropriate role for the OPC in identifying countries that have equivalent *Privacy Act* protection for personal information. Is the suggestion to seek independent legal advice a viable option?

Question 13–3 What role, if any, should the Office of the Privacy Commissioner play in identifying countries that have equivalent *Privacy Act* protection for personal information?

Requirement of notice that information is being sent overseas

13.44 The OPC Review noted that, in its stakeholder consultations, many consumers expressed concerns about the use of overseas call centres by Australian businesses. For many consumers 'the transfer of personal information overseas brings with it a perceived loss of privacy and control'.[46]

13.45 In its submission to the OPC Review, Electronic Frontiers 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.[47]

13.46 As part of this notice, Electronic Frontiers argued that organisations should also be required to inform individuals of the means by which the Australian organisation has ensured that its personal information will be adequately protected. Such notice would not be required if the overseas organisation is subject to substantially similar

---

44 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 78.
45 Ibid, Rec 18.
46 Ibid, 78.
47 Ibid, 78.

privacy laws or the individual has consented to the transfer.[48] This suggestion was not discussed further in either the OPC Review or the Senate Committee privacy inquiry.

13.47 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'.[49] Under cl 10(b)(1) of the Bill, 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 employing people in this very lucrative, rapidly growing area of information handling, they need to strengthen their own laws.[50]

13.48 This aspect of the Bill has been criticised as an unnecessary burden on business. In the US context, the example was cited of a company with data processing centres in the USA 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.[51]

13.49 The form in which the notice should be given is an issue in terms of the burden it would place on business. There is an enormous cost difference depending on whether notice has to be given to each individual or whether it could, for example, be posted on a company website. In consultations in the course of this Inquiry it was noted that for large companies, the cost of complying with the requirement to give individual notice can run to millions of dollars.[52]

Question 13–4 Should organisations be required to inform individuals that their personal information is to be transferred outside Australia? If so, what form should such notification take?

---

48 Ibid, 79.

49 The text of the Bill may be viewed at <www.theorator.com/bills109/s3713.html> (6 September 2006). The Bill has been sent to the Senate Judiciary Committee for consideration.

50 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 11 September 2006.

51 K Magill, 'Hillary's Privacy Bill a Whopper', *Direct Magazine* (online), 5 September 2006, <directmag.com/news/hillary_privacy_bill>.

52 A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

European Union Data Protection Directive

13.50 The EU Directive has an impact on Australian privacy law, as it gives Europeans privacy protection rights when information about them is transferred to countries outside the European Union.[53] 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.[54]

13.51 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.

13.52 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.

13.53 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;
- 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.

13.54 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'.

---

53 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).

54 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), 9.

13.55 The decision as to 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 Harbor Privacy Principles has also been given adequacy status.[55]

13.56 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'.[56]

13.57 If a third country is deemed not to have adequate protection, member states must take action to prevent any transfer of data to the country in question. This 'mandated approach' is stronger than that set out in the OECD Guidelines.[57]

13.58 Bennett and Raab note that the implementation of arts 25 and 26 pose problems for businesses that rely on transborder flows of personal data. It 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 worldwide.[58]

Adequacy of the Privacy Act

13.59 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.[59] 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 data.[60] The Working Party found that, without further safeguards, this prevented the Australian standards from being deemed equivalent to the EU Directive. The Working Party also expressed concerns about Australia's regulation of sensitive

---

55 See http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm (30 August 2006).

56 Text on Non-Discrimination adopted by the Article 31 Committee (31 May 2000); cited in D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 935.

57 C Bennett and C Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (2006), 99.

58 Ibid, 99.

59 Revised Explanatory Memorandum, Privacy Amendment (Private Sector) Bill 2000 (Cth), 11–12.

60 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.

information within the *Privacy Act* and the lack of correction rights, which existed for European Union citizens under the Act.[61]

13.60 Further amendments were made to the *Privacy Act* in April 2004 as part of the process of moving towards compliance.[62] 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.[63]

13.61 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*.[64] In evidence to the Senate Committee privacy inquiry the Attorney-General's Department noted that the small business exemption is the key outstanding issue to be resolved with the European Union.[65]

13.62 There is no equivalent in the EU Directive for an 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.[66]

13.63 In evidence to the Senate Committee privacy inquiry, the Law Institute of Victoria outlined its concerns arising from the lack of compliance with the EU Directive.

> In terms of business, our submission deals with the need for Australia to have a privacy system that complies with the EU directive. It is particularly important for Australian businesses that are collecting information and want to deal transnationally. If we do not comply with the EU directive, Australian businesses are going to be

---

61 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.

62 *Privacy Amendment Act 2004* (Cth).

63 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 74.

64 Ibid, 74.

65 Commonwealth of Australia, *Parliamentary Debates*, Senate Legal and Constitutional References Committee, 19 May 2005, 63 (C Minihan). The small business exemption is discussed further in Ch 5.

66 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.

> impacted in terms of the extent to which they can work offshore and deal with other jurisdictions.[67]

13.64 This view was not shared, however, by a number of other 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. This view was shared by the Privacy Commissioner, who stated that, in practice, businesses simply included the relevant privacy standards in contracts.[68] The issue of contracts is discussed further below.

13.65 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'.[69]

13.66 Notwithstanding the evidence that this has not had a significant impact on businesses trading with the EU, the Senate Committee privacy inquiry also considered it desirable for Australia's privacy laws to be recognised as 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.[70]

13.67 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.

The use of contracts for compliance with the EU Directive

13.68 Contracts have been recognised as a mechanism for enhancing privacy protection alongside laws and self-regulatory arrangements.[71] 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

---

67 Ibid, [4.127].

68 Ibid, [4.130]. This view was also shared in consultations with the ALRC: A Beatty, A Smith and J Moore, *Consultation PC 7*, Sydney, 7 March 2006.

69 However, the Review concluded 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.

70 Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005), Rec 16.

71 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.

the data to meet the EU standards of information practices, such as the right to notice, consent, access and legal remedies.[72]

13.69 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.[73]

13.70 The Australian Bankers Association submitted to the OPC Review that:

> Ideally, the ABA would like to see the Commonwealth Government continue to press the EU for 'adequacy' recognition but not at the expense of the flexibility and 'light touch' nature of the regime. In the meantime the OFPC could give consideration to the development of standard terms contractual clauses that meet the requirements of Article 26 and that those standard clauses are publicly available for the use of organisations in appropriate circumstances.[74]

13.71 ADMA also submitted to the OPC Review that it would be beneficial for standard contracts to be made readily available to assist organisations transferring data to or from the EU or APEC regions.[75]

13.72 The ALRC is interested in hearing whether it is necessary and desirable for the *Privacy Act* to be recognised as adequate within the meaning of the EU Directive. If so, what measures are necessary to ensure the adequacy of Australia's privacy regime under the EU Directive. For example, is removal or amendment of the small business exemption and the employee records exemption desirable in this context?[76] Would the

---

72 South African Law Reform Commission, *Privacy and Data Protection*, Discussion Paper 109 (2005), 361.

73 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.

74 Australian Bankers Association, *Submission to Review of the Private Sector Provisions of the Privacy Act*, 22 December 2004.

75 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.

76 See Ch 5, Question 5–6.

availability of standard contractual clauses be sufficient to meet the needs of Australian businesses in this regard?

Question 13–5 Is adequacy of the *Privacy Act* under the European Union Data Protection Directive: (a) necessary for the effective conduct of business with European Union members; and (b) desirable for the effective protection of personal information transferred into and out of Australia? If so, what measures are necessary to ensure the adequacy of Australia's privacy regime under the European Union Data Protection Directive?

Asia-Pacific Economic Co-operation Privacy Framework

13.73 The APEC Privacy Framework was endorsed by APEC Ministers in November 2004.[77] 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'.[78]

13.74 Like 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.[79] Unlike the EU Directive, however, APEC members are not obliged to implement the APEC Privacy Framework in any particular way domestically.[80]

> Implementation measures will vary as between economies and the steps that are required in any particular economy can only be determined by that economy. Some assistance in domestic and international implementation has been provided and more may be available if required.[81]

13.75 APEC commenced development of the APEC Privacy Framework in 2003. The APEC Privacy Framework 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.

13.76 As noted in Chapter 4, the APEC principles are intended to apply to persons or organisations in both the public and private sectors who control the collection, holding,

---

77 The Asia-Pacific Economic Cooperation forum comprises 21 economies around the Pacific Ocean, including the United States, Canada, China, Japan, South Korea and Australia.

78 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), foreword. The APEC Privacy Framework is also discussed in Ch 4.

79 Ibid, [5]–[6].

80 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor*.

81 Ibid.

use, transfer or disclosure of personal information.[82] The principles cover: preventing harm; notice; collection limitation; use of personal information; choice; integrity of personal information; security safeguards; access and correction; and accountability.[83] The principles are intended to serve as the foundation for encouraging the development of appropriate information privacy protections by members.[84] Chapter 4 outlines in more detail the general differences between the APEC Privacy Framework, the EU Directive and the IPPs and NPPs under the *Privacy Act.*

13.77 One key area where the APEC Privacy Framework takes a different approach to the EU Directive is in terms of 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.[85]

13.78 While the EU Directive is concerned with border controls and whether the 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.[86]

13.79 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.

13.80 Principle 9 is therefore similar to NPP 9 in that it also uses the term 'reasonable steps'. However, the reference to 'due diligence' may be perceived as stronger than the requirement of 'reasonable belief' in NPP 9.

13.81 Given the vast differences between the member states of APEC, the APEC Privacy Framework does not aspire to uniformity but strives to recognise cultural and other diversities within member economies.[87] The APEC Privacy Framework's

---

82 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [10].
83 See Ibid, [14]–[26].
84 Ibid, preamble.
85 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor*, 8.
86 Ibid.
87 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [5]–[6].

approach to transborder data protection is to encourage cooperation between members on the regional enforcement of data protection norms and the development of agreements between nations for cooperative enforcement.[88] These cross-border arrangements may include mechanisms:

- for notifying public authorities in other member states of investigations and assistance in investigations; and

- to identify and prioritise cases for cooperation in severe cases of privacy infringement that may involve authorities in several countries.[89]

13.82 APEC members have also agreed to support the development and recognition of members' cross-border privacy rules 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.[90]

13.83 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.[91]

13.84 The APEC Privacy Framework has been criticised, however, as being too 'light touch' in its approach and in not providing sufficient privacy protection for individuals. Professor Greenleaf argues that the APEC Privacy Framework has a bias towards the free flow of information and does not recognise that there can be legitimate privacy reasons for restricting data exports.[92] The requirement of either consent or that the discloser takes reasonable steps to protect the information is, in Professor Greenleaf's

---

88 M Crompton and P Ford, 'Implementing the APEC Privacy Framework: A New Approach' (2005) 5(15) *IAPP Privacy Advisor*, 8.

89 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [46]. The issue of the need for more cross-border investigations of privacy breaches and the improved transfer of data between jurisdictions for investigatory purposes was raised in consultation: P Cullen, T Hughes and M Crompton, *Consultation*, Sydney, 8 May 2006.

90 Asia-Pacific Economic Cooperation, *APEC Privacy Framework* (2005), [48].

91 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), 75.

92 G Greenleaf, 'APEC's Privacy Framework: A New Low Standard' (2005) 11 *Privacy Law & Policy Reporter* 121, 122.

view, 'a very soft substitute for a Data Export Limitation principle' along the lines of that contained in the EU Directive.[93]

13.85 Professor 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.[94]

Asia-Pacific Privacy Charter Initiative

13.86 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.[95] 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.[96]

13.87 The general principles cover justification and proportionality, consent, accountability, openness, non-discrimination, and reasons for non-compliance.[97] There are 13 information privacy principles covering: anonymous transactions, collection limitation, identifier limitation, information quality, use and disclosure limitations, export limitations, access and correction, retention limitation, public registers, information security, automated decisions, identity protection and disclosure of private facts.[98]

13.88 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.[99] However, the APP Charter, as it stands, is intended to be a 'maximalist' or 'high watermark' draft, reflecting all the significant privacy principles from relevant international instruments.[100] Two examples where the APP Charter takes a stronger approach than the APEC Privacy Framework are:

---

93 Ibid, 125.

94 G Greenleaf, 'APEC Privacy Framework Completed: No Threat to Privacy Standards' (2006) *Privacy Law & Policy Reporter* 5.

95 Cyberspace Law and Policy Centre, 'Announcement: Asia-Pacific Privacy Charter Initiative' (Press Release, 1 May 2003). As at 1 September 2006, a second draft of the Charter had not yet been released for public comment.

96 See Ibid. The Charter is also discussed in Ch 4.

97 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 11 September 2006, Principles 1–6.

98 Ibid, Principles 7–19. As well as Information Privacy Principles, the APP Charter also contains Surveillance Limitation Principles, Intrusion Limitation Principles, and Implementation and Compliance Principles.

99 Ibid, 1.

100 Ibid, 1.

- *Notice*: Principle 2 of the APEC Privacy Framework requires that notice of the purpose of collection and other matters must be given by 'clear and easily accessible' statements, but does not specify that it should be by notice to individuals. Under Principle 8 of the APP Charter, notice must be given to the person concerned.

- *Uses of personal information*: Principle 4 of the APEC Privacy Framework states that personal information collected should only be used to fulfil the purposes of collection and other compatible or related purposes. The APP Charter suggests a stricter test on secondary use, being for a purpose directly related to the purpose of the collection and within the reasonable expectations of the person concerned.[101]

13.89 In relation to transborder data flows, as noted above, 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

- 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.

13.90 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 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.

Question 13–6 Does the APEC Privacy Framework provide an appropriate model for the protection of personal information transferred between countries? Are other standards, such as the Asia-Pacific Charter, a more appropriate model?

101 Ibid, pt II, IPP 11. This is similar to NPP 2.1(a) under the *Privacy Act.*

Other international models

13.91 This section considers other international models for the regulation of transborder data flows.[102] The United States Safe Harbor arrangements and the privacy regimes of Canada and Argentina have been approved by the European Commission as adequate for the purpose of the EU Directive. The example of an EU country (Germany) is also given. Finally, the chapter considers the developing system of data protection in India.

US Safe Harbor arrangements

13.92 As noted elsewhere in this Issues Paper, there are substantial differences between the European approach to information privacy and the approach taken in the United States. Given the lack of an overarching privacy regime in the United States, in 1998 the US Department of Commerce began negotiations with the EU Commission to develop an opt-in 'safe harbor' scheme to ensure that the US could meet the test of adequacy in art 25.[103]

13.93 The Safe Harbor framework allows individual companies to elect to adhere to seven principles. The principles are:

> *Notice:* An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure.
>
> *Choice:* An organization must offer individuals the opportunity to choose (opt-out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual.
>
> *Onward transfer:* To disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either ascertains that the third party subscribes to the safe harbour principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.
>
> *Security:* Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.
>
> *Data integrity:* Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. To the extent necessary for those purposes,

---

102 Other aspects of these countries' privacy regimes are discussed in Ch 4.

103 D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 938.

> an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
>
> *Access:* Individuals must have access to personal information about them that an organization holds and be able to correct, amend**,** or delete that information where it is inaccurate.
>
> *Enforcement:* Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed.[104]

13.94 The US Department of Commerce website indicates that over 1000 companies have now signed up to the principles. The Safe Harbor principles are enforced via a 'self regulatory' approach, which encourages adopting organisations to have internal dispute resolution mechanisms. Given that the United States does not have a privacy regulator to enforce privacy law, federal and state laws relating to unfair and deceptive acts apply to organisations that fail to adhere to the principles once adopted.[105]

13.95 The Safe Harbor principles have been criticised on the basis that they: create two systems of data collection for companies that collect personal data from both the United States and the EU; and that there is no judicial remedy available for breaches under the Safe Harbor principles.[106]

13.96 The absence of a federal privacy regulator in the United States also places a burden on the individual to enforce their rights.

> It is up to him to verify whether the American body which deals with the data is in a position of compliance or not, it is up to him to find, and to refer the matter to, the appropriate independent control authority to study his case, it is up to him to put forward the arguments of his application.[107]

13.97 On this basis, it could be argued that Australia's privacy regime provides a level of protection that is higher than that in the United States as it offers a conciliation system for resolution of complaints, recourse to the courts for individuals and a federal Privacy Commissioner to oversee implementation. However, in terms of the substance of the rules, the Safe Harbor principles do not have the same exemptions as the *Privacy Act* and therefore arguably their scope is more comprehensive.[108]

---

104 United States Government Department of Commerce, *Safe Harbor Privacy Principles* (2000).

105 K Sainty and A Ailwood, *Managing Compliance in the Global Space—Transborder Data Flow* (2004) Allens Arthur Robinson, 6.

106 D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 950.

107 Yves Poullet, *The Safe Harbor Principles: An Adequate Protection?* (June 2000), cited in Ibid, 953. The Federal Trade Commission does have a role in investigating claims made by business about their privacy protections.

108 A Hughes, 'A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)' (2001) 24 *University of New South Wales Law Journal* 270, 275.

Canada

13.98 The *Personal Information Protection and Electronic Documents Act* (2000) (PIPED Act) applies to organisations in respect of personal information that they collect, use or disclose in the course of commercial activities, or certain personal information about their employees.[109] Subject to certain exceptions, the PIPED Act requires organisations to comply with the *National Standard of Canada Model Code for the Protection of Personal Information* (Model Code), which is a schedule to the Act.[110] The Model Code sets out ten key principles which cover accountability; identifying purposes; consent; collection; use, disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance. Details of the Canadian regime are discussed in Chapter 4.

13.99 Under Principle 4.1.3 of the Model Code, 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. Organisations must use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. Canadian companies must therefore incorporate the PIPED Act's privacy requirements into all contracts that contemplate the transfer of Canadians' personal information to foreign companies.[111]

13.100 In 2001, the EU Commission issued a decision that the PIPED Act provides an adequate level of protection for the purpose of the EU Directive.

> The Canadian Act covers all the basic principles necessary for an adequate level of protection for natural persons, even if exceptions and limitations are also provided for in order to safeguard important public interests and to recognise certain information which exists in the public domain. The application of these standards is guaranteed by judicial remedy and by independent supervision carried out by the authorities, such as the Federal Privacy Commissioner invested with powers of investigation and intervention. Furthermore, the provisions of Canadian law regarding civil liability apply in the event of unlawful processing which is prejudicial to the persons concerned.[112]

13.101 The Canadian Government has also recently released a new federal strategy for protecting privacy rights where personal information is being handled by a foreign government. This is a response to concerns that information about Canadian citizens—for example, credit card details—that is stored in the United States may be subject to

---

109 *Personal Information Protection and Electronic Documents Act 2000* RS 2000, c 5 (Canada) s 4(1).

110 Ibid s 5.

111 D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 923.

112 Commission of the European Communities, *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data provided by the Canadian Personal Information Protection and Electronic Documents Act*, 2002/2/EC (2001).

the PATRIOT Act.[113] The strategy involves raising awareness among Canadian government departments about the risks of outsourcing information to the United States, and developing strategies to minimise potential privacy risks when considering future contracts or action.[114]

Argentina

13.102 In 2000, Argentina enacted the Law for the Protection of Personal Data. The Law is based on the EU Directive, parts of the *Argentinean Constitution*, and some early laws relating to privacy. Under the Law, international transfer of personal information is prohibited to countries without adequate protection.[115] On this basis the European Commission has determined that Argentina provides an adequate level of protection for the purposes of the EU Directive.[116]

Germany

13.103 As noted in Chapter 4, the *Federal Data Protection Act 1990* (Germany) (FDP Act) does not adopt principles, as such, in protecting personal data in the various stages of the information cycle. Part I of the FDP Act contains provisions applicable to both the public and private sectors. Section 4b covers transborder data flows. Under s 4b(2), the transfer of information to foreign bodies must not take place where the bodies in question do not offer an adequate level of data protection.[117] Transfers may be allowed, even if the protection is not adequate, on the same terms as contained in the EU Directive. For example, transfers of data may occur where the individual has given consent, the transfer is necessary for the performance of a contract, or is necessary in order to protect the vital interests of the individual.[118]

India

13.104 India is currently the largest host of outsourced data processing in the world. Some estimates claim that India hosts 44% of the global market of outsourced software and 'back-office' services.[119]

---

113 *Uniting and Strengthening America by Providing the Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001* (US). The Act allows US law enforcement officers to access information about individuals without their knowledge: 'Canada Seeks to Protect Citizens' Privacy' (2006) (July/August) *Information Management Journal* 18, 18.

114 Treasury Board of Canada, *Privacy Matters: The Federal Strategy to Address Concerns About the US PATRIOT Act and Transborder Data Flows* (2006), 1.

115 D Solove, M Rotenberg and P Shwartz, *Information Privacy Law* (2nd ed, 2006), 929.

116 See European Commission *Opinion 4/2002 on the Level Of Protection Of Personal Data in Argentina* <//ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp63_en.pdf> (9 September 2006).

117 An exception is made to this principle where the transfer is necessary for the discharge of a federal public body's own duties on urgent grounds of security or for the performance of multilateral or bilateral obligations in the area of crisis management or conflict prevention or for humanitarian measures; *Federal Data Protection Act 1990* (Germany) s 4b(2).

118 Ibid s 4c.

119 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.

13.105 Currently, no data privacy protection legislation is in place in India. Outsourcing countries, like the United States and Australia, rely on contractual obligations and the internal measures taken by Indian companies.[120] Given the extent to which India is used as an outsourcing destination, data protection has become a political issue in the region. The adoption of model legislation based on the EU Directive has been proposed in the past; however, the Indian Government has given some indication that it may adopt a model closer to the United States Safe Harbor principles, as a simpler regulatory solution.[121]

120 Ibid, 13.

121 K Sainty and A Ailwood, *Managing Compliance in the Global Space—Transborder Data Flow* (2004) Allens Arthur Robinson, 7.

Appendix 1. List of Submissions

Name	*Submission Number*	*Date*
S Alexander	PR 51	18 August 2006
Anonymous	PR 22	20 June 2006
D Antulov	PR 14	28 May 2006
Australian Press Council	PR 48	8 August 2006
P Baum	PR 34	1 June 2006
L Bennett	PR 21	11 June 2006
K Bottomley	PR 10	1 May 2006
J Carland and J Pagan	PR 42	11 July 2006
Chocolate Messages Pty Ltd	PR 9	1 June 2006
Community Services Ministers' Advisory Council	PR 47	28 July 2006
Confidential	PR 5	3 April 2006
Confidential	PR 6	6 March 2006
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

Name	*Submission Number*	*Date*
Confidential	PR 49	14 August 2006
Consumer Credit Legal Centre (NSW) Inc	PR 28	6 June 2006
S Crothers	PR 43	14 July 2006
I Cunliffe	PR 37	9 May 2006
T de Koke	PR 8	5 April 2006
W Dowdell	PR 1	16 February 2006
J Dowse	PR 44	2 June 2006
Dun & Bradstreet	PR 11	13 April 2006
Edentiti	PR 29	3 June 2006
H Fleming	PR 38	27 June 2006
K Gardiner	PR 33	1 June 2006
K Handscombe	PR 52	13 September 2006
J Harvey	PR 12	25 May 2006
M Hunter	PR 16	1 June 2006
J Kerr	PR 4	13 March 2006
P Lee-Archer	PR 20	2 June 2006
Link Market Service	PR 2	24 February 2006
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
L Mitchell	PR 46	2 June 2006

Name	***Submission Number***	***Date***
S Newton	PR 23	8 June 2006
L O'Connor	PR 35	2 June 2006
J Partridge	PR 26	4 June 2006
F Pilcher	PR 17	1 June 2006
Real Estate Institute of Australia	PR 7	10 April 2006
M Rickard	PR 19	1 June 2006
M Rosenthal	PR 50	15 August 2006
H Ruglen	PR 39	27 June 2006
Salvation Army	PR 15	2 June 2006
T Stutt and L Nicholls	PR 40	11 July 2006
C Taylor	PR 36	17 June 2006
S Tully	PR 25	7 June 2006
P Wikramanayake	PR 45	1 June 2006

Appendix 2. 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)
AAT	Administrative Appeals Tribunal
ABC	Australian Broadcasting Corporation
ABS	Australian Bureau of Statistics
ACA	Australian Communications Authority
ACC	Australian Crime Commission
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
ADMA	Australian Direct Marketing Association
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977* (Cth)
ADR	Alternative Dispute Resolution
Advisory Committee	Privacy Advisory Committee
AFP	Australian Federal Police
AGAC	Australian Guardianship and Administration Committee
AGD	Australian Government Attorney-General's Department
AHEC	Australian Health Ethics Committee

AHMAC	Australian Health Ministers' Advisory Council
AIRC	Australian Industrial Relations Commission
ALRC	Australian Law Reform Commission
ALRC 11	Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, ALRC 11 (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 Bill 2006	Revised exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth)
AML/CTF Rules	Anti-Money Laundering and Counter-Terrorism Financing Rules (Cth)
ANZDATA	Australian and New Zealand Dialysis and Transplant Registry
APC	Australian Press Council
APEC	Asia-Pacific Economic Cooperation
APF	Australian Privacy Foundation
APPA	Asia Pacific Privacy Authorities Forum
APP Charter	Asia-Pacific Privacy Charter

APPC Council	Asia-Pacific Privacy Charter Council
ARC	Administrative Review Council
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
ASSPA	Aboriginal Sacred Sites Protection Authority
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
Austrade	Australian Trade Commission
BFSO	Banking and Financial Services Ombudsman
CDE project	Census Data Enhancement project
CND	Calling Number Display
COAG	Council of Australian Governments
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)
CROC	United Nations *Convention on the Rights of the Child 1989*
CSMAC	Community Services Ministers' Advisory Council
CSIRO	Commonwealth Scientific and Industrial Research Organisation
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
DOHA	Australian Government Department of Health and Ageing
DRM	Digital Rights Management
DSD	Australian Government Defence Signals Directorate
EFA	Electronic Frontiers Australia Inc
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)
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)
FTC	United States Federal Trade Commission
GPS	Global Positioning System
HPP	Health Privacy Principle
HREC	Human Research Ethics Committee
HTTP	Hypertext Transfer Protocol
ICCPR	*International Covenant on Civil and Political Rights 1966*
IGIS	Inspector-General of Intelligence and Security

IIA	Internet Industry Association
IPND	Integrated Public Number Database
IPP	Information Privacy Principle
ISP	Internet Service Provider
MCCA	Ministerial Council on Consumer Affairs
National Archives	National Archives of Australia
National Statement	National Statement on Ethical Conduct in Research Involving Humans
NEHTA	National E-Health Transition Authority
NHMRC	National Health and Medical Research Council
NPP	National Privacy Principle
NSWLRC	New South Wales Law Reform 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)
PETs	privacy enhancing technologies
PIA	Privacy Impact Assessment
PID	Public Interest Determination

PIPED Act	*Personal Information Protection and Electronic Documents Act 2000* (Canada)
PIPP	Personal Information Protection Principle
Privacy Act	*Privacy Act 1988* (Cth)
REIA	Real Estate Institute of Australia
RFID	Radio Frequency Identification
RIS	Regulatory Impact Statement
RTD	Residential Tenancy Database
SBS	Special Broadcasting Service
SCAG	Standing Committee of Attorneys-General
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)
Senate Committee privacy inquiry	Parliament of Australia—Senate Legal and Constitutional References Committee inquiry into the *Privacy Act 1988* (Cth)
SLCD	Statistical Longitudinal Census Dataset
TFN	Tax File Number
TIO	Telecommunications Industry Ombudsman
TPID	Temporary Public Interest Determination
VLRC	Victorian Law Reform Commission
VoIP	Voice over Internet Protocol