



Australian Government  
Australian Law Reform Commission

# Review of Secrecy Laws

DISCUSSION PAPER

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

DISCUSSION PAPER 74  
JUNE 2009

This Discussion Paper reflects the law as at 1 June 2009

© Commonwealth of Australia 2009

This work is copyright. You may download, display, print and reproduce this material in whole or part, subject to acknowledgement of the source, for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the *Copyright Act 1968* (Cth), all other rights are reserved. Requests for further authorisation should be directed by letter to the Commonwealth Copyright Administration, Copyright Law Branch, Attorney-General's Department, Robert Garran Offices, National Circuit, Barton ACT 2600 or electronically via [www.ag.gov.au/cca](http://www.ag.gov.au/cca).

ISBN- 978-0-9804153-6-0

Commission Reference: DP 74

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](mailto:info@alrc.gov.au)

ALRC homepage: [www.alrc.gov.au](http://www.alrc.gov.au)

Printed by Ligare Pty Ltd

# Making a submission

---

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

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

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

## Open inquiry policy

In the interests of informed public debate, the ALRC is committed to open access to information. As submissions provide important evidence to each inquiry, it is common for the ALRC to draw upon the contents of submissions and quote from them or refer to them in publications. As part of ALRC policy, non-confidential submissions are made available to any person or organisation upon request after completion of an inquiry, and may also 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 *Freedom of Information Act 1982* (Cth), which has provisions designed to protect sensitive information given in confidence.

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

Submissions should be sent to:

The Executive Director  
Australian Law Reform Commission  
GPO Box 3708  
SYDNEY NSW 2001  
Email: [secrecy@alrc.gov.au](mailto:secrecy@alrc.gov.au)

Submissions may also be made using the online form on the ALRC's homepage:  
[<www.alrc.gov.au>](http://www.alrc.gov.au)

**The closing date for submissions in response to DP 74 is 7 August 2009.**



# Contents

---

## Contents

<b>Terms of Reference</b>	<b>5</b>
<b>List of Participants</b>	<b>7</b>
<b>List of Proposals and Questions</b>	<b>9</b>
<b>1. Introduction to the Inquiry</b>	<b>23</b>
Background	23
Scope of the Inquiry	29
Process of reform	34
Discussion Paper 74	38
<b>2. Open Government, Secrecy and Public Interest</b>	<b>43</b>
Introduction	43
Why secrecy?	44
Towards openness	46
The idea of accountability	48
Secrecy laws and the Australian Constitution	58
The public interest	71
<b>3. Sharing Commonwealth Information</b>	<b>79</b>
Introduction	79
Framework for information sharing	81
Outcomes of information sharing	90
<b>4. Freedom of Information, Privacy and Secrecy</b>	<b>105</b>
Introduction	105
Freedom of information	106
Archives	134
Privacy	143
<b>5. Overview of Current Secrecy Laws</b>	<b>153</b>
Introduction	153
Common law duties	154
Statutory secrecy provisions	161
General criminal offences	184
Comment	196

---

<b>6. The Need for a General Secrecy Offence</b>	<b>199</b>
Introduction	199
Criminal, civil or administrative penalties	200
The need for a general secrecy offence	216
<b>7. General Secrecy Offence: Harm to Public Interests</b>	<b>223</b>
Introduction	223
Duty not to disclose information	224
Harm to identified public interests	228
<b>8. General Secrecy Offence: Elements</b>	<b>259</b>
Introduction	259
Whose conduct should be regulated?	260
Initial and subsequent disclosures	276
What conduct should be regulated?	282
What information should be protected?	290
<b>9. General Secrecy Offence: Exceptions and Penalties</b>	<b>293</b>
Exceptions and defences	293
Exceptions and defences for inclusion in the general secrecy offence	295
Public interest disclosure	315
Penalties	324
Other issues	333
<b>10. Specific Secrecy Offences: Elements</b>	<b>343</b>
Introduction	343
Reasonable likelihood of harm	344
Whose conduct should be regulated?	356
What conduct should be regulated?	362
What information should be protected?	368
<b>11. Specific Secrecy Offences: Exceptions and Penalties</b>	<b>373</b>
Introduction	373
Exceptions and defences	373
Penalties	389
Consistency of penalties	395
Level of maximum penalty	404
<b>12. Specific Secrecy Offences: Simplification and Consistency</b>	<b>413</b>
Introduction	413
Replication of secrecy offences	414
Identifying examples of substantial replication	419
Case study: <i>Crimes Act 1914 (Cth) s 79</i>	425
Consistency in secrecy offences	433
Consolidation of secrecy offences	436
Implementation	439

<b>13. Administrative Obligations in the Australian Public Service</b>	<b>443</b>
Introduction	443
The Australian Public Service	444
Framework for secrecy obligations in the APS	445
Prejudice to the effective working of government	450
Information communicated in confidence	464
Exceptions and defences	466
Penalties	469
Processes for dealing with breaches	472
<b>14. Regulating Beyond the <i>Public Service Act</i></b>	<b>483</b>
Introduction	483
Commonwealth employees outside the APS	484
Former Commonwealth employees	499
Persons outside Commonwealth employment	503
Lawful and reasonable employer directions	519
<b>15. Fostering Effective Information-Handling Practices</b>	<b>523</b>
Introduction	523
An effective information-handling culture	524
Risk factors for inappropriate information handling	525
Agency policies and guidelines	526
Memorandums of understanding	533
Training and development programs	536
Oaths, affirmations and acknowledgements of secrecy	539
Information and communication technology systems	542
Avenues for employee queries and concerns	544
Fostering effective information handling at the agency level	546
Fostering effective information handling in the private sector	554
<b>Appendix 1. List of Submissions</b>	<b>557</b>
<b>Appendix 2. List of Agencies, Organisations and Individuals Consulted</b>	<b>561</b>
<b>Appendix 3. List of Abbreviations</b>	<b>563</b>
<b>Appendix 4. Table of Secrecy Provisions</b>	<b>569</b>
<b>Appendix 5. Extracts of Key Secrecy Provisions</b>	<b>583</b>



# **Terms of Reference**

---

## **REVIEW OF SECRECY LAWS**

I, ROBERT McCLELLAND, Attorney-General of Australia, having regard to:

- the desirability of having comprehensive, consistent and workable laws and practices in relation to the protection of Commonwealth information;
- the increased need to share such information within and between governments and with the private sector;
- the importance of balancing the need to protect Commonwealth information and the public interest in an open and accountable system of government; and
- previous reports (including previous reports of the Commission) that have identified the need for reform in this area

REFER to the Australian Law Reform Commission for inquiry and report, pursuant to subsection 20(1) of the *Australian Law Reform Commission Act 1996*, options for ensuring a consistent approach across government to the protection of Commonwealth information, balanced against the need to maintain an open and accountable government through providing appropriate access to information.

1. In carrying out its review, the Commission will consider:
  - a. relevant laws and practices relating to the protection of Commonwealth information, including the scope and appropriateness of legislative provisions regarding secrecy and confidentiality;
  - b. whether there is a need to consolidate and modernise relevant provisions currently in the *Crimes Act 1914* and other Commonwealth legislation for inclusion in the *Criminal Code*;
  - c. the way in which secrecy laws in the *Crimes Act* interact with other laws and practices, including those relating to secrecy, privacy, freedom of information, archiving, whistle-blowing, and data-matching;
  - d. whether there should be different considerations for secrecy laws relating to the protection of national security and other sensitive Commonwealth information; and
  - e. any related matter.

2. In carrying out its review, the Commission is to identify and consult with key stakeholders, including relevant Commonwealth, State and Territory agencies and private sector bodies.
3. The Commission will provide its final report to me by 31 October 2009.

Dated 5 August 2008

Robert McClelland

Attorney-General

# List of Participants

---

## Australian Law Reform Commission

### Division

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

Professor David Weisbrot (President)  
Professor Les McCrimmon (Commissioner)  
Professor Rosalind Croucher (Commissioner in charge)  
Justice Berna Collier (part-time Commissioner)  
Justice Susan Kenny (part-time Commissioner)

### Senior Legal Officers

Carolyn Adams  
Bruce Alston

### Legal Officers

Anna Dziedzic  
Lisa Eckstein

### Consultant

Amie Grierson

### Research Manager

Jonathan Dobinson

### Librarian

Carolyn Kearney

### Project Assistant

Tina O'Brien

### Legal Interns

Michael Evry  
Stephanie Fusco  
Kelvin Liew  
Isley Markman  
Katy McGree  
Larisa Michalko

Tracy Nau  
Naomi Oreb  
Christina Ray  
Katie Schafer  
Michael Wells  
Smriti Sriram  
Yi-Shun Teoh  
Rebecca Zaman

### **Advisory Committee Members**

Ms Lynelle Briggs, Australian Public Service Commissioner  
Mr Ian Carnell, Inspector-General of Intelligence and Security  
Mr Chris Craigie SC, Commonwealth Director of Public Prosecutions  
Professor Robin Creyke, College of Law, Australian National University  
Mr Simon Daley, Australian Government Solicitor  
Mr Chris Erskine SC, Blackburn Chambers  
Justice Paul Finn, Federal Court of Australia  
Mr Kevin Fitzpatrick, Chief Tax Counsel, Australian Taxation Office  
Mr Stephen Gageler SC, Solicitor-General of Australia  
Mr John McGinness, Director, National Judicial College of Australia  
Professor John McMillan, Commonwealth Ombudsman  
Mr Andrew Metcalfe, Secretary, Department of Immigration and Citizenship  
Associate Professor Moira Patterson, Law Faculty, Monash University  
Mr Peter Timmins, Timmins Consulting  
Ms Annette Willing, Australian Government, Attorney-General's Department

## List of Proposals and Questions

---

### 4. Freedom of Information, Privacy and Secrecy

**Proposal 4–1** Reflecting a commitment to open government and to ensure that claims for exemption be considered on a case by case basis rather than through the mechanism of a global exemption for secrecy provisions, s 38 of the *Freedom of Information Act 1982* (Cth) should be repealed.

**Proposal 4–2** The Office of Parliamentary Counsel should issue a Drafting Direction that any proposed secrecy provision must indicate expressly whether it overrides the *Freedom of Information Act 1982* (Cth).

**Proposal 4–3** If s 38 of the *Freedom of Information Act 1982* (Cth) is repealed, the *FOI Guidelines—Exemption Sections in the FOI Act* issued by the Department of the Prime Minister and Cabinet or the proposed Information Commissioner Guidelines should be updated to inform Freedom of Information officers that the existence of a secrecy provision is a relevant factor to consider when deciding whether or not to disclose a document.

**Proposal 4–4** If s 38 of the *Freedom of Information Act 1982* (Cth) is retained, the responsible minister (or the proposed Freedom of Information Commissioner) should ensure that the list of secrecy provisions in sch 3 of the Act is regularly reviewed and updated.

**Proposal 4–5** Complementing the idea of access that underpins both the *Archives Act 1983* (Cth) and the *Freedom of Information Act 1982* (Cth), s 33(3) of the *Archives Act* should be repealed.

**Proposal 4–6** The *Archives Act 1983* (Cth) should be amended to include a provision modelled on s 59, to the effect that where a record enters the open access period, any non-disclosure provision applicable to the record ceases to have effect, unless expressly stated in the relevant legislation.

**Proposal 4–7** The Office of Parliamentary Counsel should issue a Drafting Direction that any proposed non-disclosure provision should indicate expressly whether it overrides the *Archives Act 1983* (Cth) in the open access period.

## 6. The Need for a General Secrecy Offence

**Proposal 6–1** Sections 70 and 79(3) of the *Crimes Act 1914* (Cth) should be repealed and replaced by a new offence in the *Criminal Code* (Cth), which regulates the disclosure of Commonwealth information by Commonwealth officers (the ‘general secrecy offence’).

## 7. General Secrecy Offence: Harm to Public Interests

**Proposal 7–1** The proposed general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:

- (a) harm the national security, defence or international relations of the Commonwealth;
- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
- (c) endanger the life or physical safety of any person;
- (d) pose a serious threat to public health or public safety;
- (e) have a substantial adverse effect on personal privacy; or
- (f) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.

**Proposal 7–2** The proposed general secrecy offence should consist of three tiers, as follows:

- (a) **First tier:** the unauthorised disclosure caused, or was reasonably likely to cause, harm to one or more of the specified public interests. Strict liability attaches to this result.
- (b) **Second tier:** the Commonwealth officer was reckless as to whether, or knew or intended that, the disclosure would:
  - (i) have a substantial adverse effect on personal privacy; or
  - (ii) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.

- (c) **Third tier:** the Commonwealth officer was reckless as to whether, or knew or intended that, the disclosure would:
- (i) harm the national security, defence or international relations of the Commonwealth;
  - (ii) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
  - (iii) endanger the life or physical safety of any person; or
  - (iv) pose a serious threat to public health or public safety.

**Proposal 7–3** The first tier offence should include a defence in circumstances where the Commonwealth officer can prove that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to harm any of the specified public interests.

## 8. General Secrecy Offence: Elements

**Proposal 8–1** The proposed general secrecy offence should regulate the conduct of those who are, or have been, ‘Commonwealth officers’; defined as follows:

- (a) the Governor-General;
- (b) ministers and parliamentary secretaries;
- (c) Australian Public Service employees, that is, individuals appointed or engaged under the *Public Service Act 1999* (Cth);
- (d) individuals employed by the Commonwealth otherwise than under the *Public Service Act*;
- (e) members of the Australian Defence Force;
- (f) members or special members of the Australian Federal Police;
- (g) individuals who hold or perform the duties of an office established by or under a law of the Commonwealth;
- (h) officers or employees of Commonwealth authorities;

- 
- (i) individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth;
  - (j) individuals and entities who are contracted service providers for a Commonwealth contract; and
  - (k) individuals who are officers or employees of a contracted service provider for a Commonwealth contract and who provide services for the purposes (whether direct or indirect) of the Commonwealth contract.

**Proposal 8–2** The proposed general secrecy offence should *not* regulate the conduct of judicial officers exercising the judicial power of the Commonwealth, or Members of the Australian Parliament who are not ministers or parliamentary secretaries.

**Proposal 8–3** There should be a new offence in the *Criminal Code* (Cth) (the ‘subsequent disclosure offence’) for subsequent disclosure of Commonwealth information by any person where:

- (a) the information has been disclosed by a Commonwealth officer in breach of the proposed general secrecy offence; and
- (b) the person knows, or is reckless as to whether, the information has been disclosed in breach of the proposed general secrecy offence; and
- (c) the person knows, intends, or is reckless as to whether, the subsequent disclosure of the information will harm, or is reasonably likely to harm, one of the public interests set out in Proposal 7–1.

**Proposal 8–4** The proposed subsequent disclosure offence should include an express exception where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.

**Proposal 8–5** The proposed general secrecy offence should regulate the disclosure of Commonwealth information. The fault element attaching to disclosure should be intention.

**Proposal 8–6** The proposed general secrecy offence should apply to any information to which a person has, or had, access by reason of his or her being, or having been, a Commonwealth officer as defined in Proposal 8–1.

## 9. General Secrecy Offence: Exceptions and Penalties

**Proposal 9–1** The proposed general secrecy offence should expressly include exceptions applying where the disclosure is:

- (a) in the course of a Commonwealth officer's functions or duties;
- (b) authorised by the relevant agency head or minister, and the agency head or minister certifies that the disclosure is in the public interest; or
- (c) of information that is already in the public domain as the result of a lawful disclosure.

**Proposal 9–2** The proposed general secrecy offence should include a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.

**Proposal 9–3** The general secrecy offence should have three tiers and three penalty levels:

- (a) Where strict liability attaches to the requirement to prove harm, the penalty should be a maximum of two years imprisonment, or a pecuniary penalty not exceeding 120 penalty units, or both.
- (b) Where a Commonwealth officer knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:
  - (i) have a substantial adverse effect on personal privacy; or
  - (ii) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation,

the penalty should be a maximum of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both.

- (c) Where a Commonwealth officer knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:
  - (i) harm the national security, defence or international relations of the Commonwealth;

- (ii) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
- (iii) endanger the life or physical safety of any person; or
- (iv) pose a serious threat to public health or public safety

the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.

**Proposal 9–4** Where a person knows that, or was reckless as to whether, Commonwealth information has been disclosed in breach of the general secrecy offence, and then discloses that information knowing, or reckless as to whether, or intending that the subsequent disclosure of Commonwealth information will:

- (a) have a substantial adverse effect on personal privacy; or
- (b) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation,

the penalty should be a maximum of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both.

**Proposal 9–5** Where a person knows that, or was reckless as to whether, Commonwealth information has been disclosed in breach of the general secrecy offence, and then discloses that information knowing, or reckless as to whether, or intending that the subsequent disclosure of Commonwealth information will:

- (a) harm the national security, defence or international relations of the Commonwealth;
- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
- (c) endanger the life or physical safety of any person; or
- (d) pose a serious threat to public health or public safety,

the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.

**Proposal 9–6** The proposed general secrecy offence, and the subsequent disclosure offence, should provide that, where a court is satisfied that a person has disclosed, or is about to disclose, information in contravention of the provisions, the court may grant an injunction to restrain such disclosure.

## 10. Specific Secrecy Offences: Elements

**Proposal 10–1** Specific secrecy offences should generally incorporate a requirement that, for an offence to be committed, there must be a reasonable likelihood that the disclosure of information will cause harm to some specified public interest, except where there are clear countervailing public interests.

**Question 10–1** In what circumstances is it inappropriate for a secrecy offence to require that a disclosure be reasonably likely to cause harm—for example, in relation to the disclosure of national security classified information or information concerning the defence or international relations of the Commonwealth?

**Proposal 10–2** (a) Where specific secrecy offences incorporate a reasonable likelihood of harm requirement, recklessness should generally be the fault element for offences punishable by imprisonment for more than a maximum of two years.

(b) For other offences, strict liability should apply in relation to the likelihood of harm.

**Proposal 10–3** Specific secrecy offences that are stated to apply to ‘any person’ should be reviewed to establish whether the offences should apply only to ‘Commonwealth officers’ and to subsequent disclosure, as defined in the general secrecy offence and the subsequent disclosure offence (Proposals 8–1, 8–3).

**Proposal 10–4** Specific secrecy offences that apply to Commonwealth officers should be reviewed to establish whether the offences should be stated to apply also to former Commonwealth officers.

**Proposal 10–5** Specific secrecy offences should generally not extend to conduct other than the disclosure of information, such as making a record, receiving or possessing protected information.

**Proposal 10–6** Specific secrecy offences should generally require intention as the fault element for the disclosure of information.

**Proposal 10–7** Specific secrecy offences that provide that strict liability applies to one or all physical elements should be reviewed to establish whether the application of strict liability remains justified.

**Proposal 10–8** Specific secrecy offences that apply to Commonwealth officers should generally apply to all information to which a Commonwealth officer has, or had, access by reason of being a Commonwealth officer.

## 11. Specific Secrecy Offences: Exceptions and Penalties

**Proposal 11–1** Specific secrecy offences that include defences should be reviewed to assess whether these defences are appropriate, in view of the general principles of criminal responsibility set out in ch 2 of the *Criminal Code*. Where such a defence is found to be appropriate, consideration should be given to recasting the provision as an exception, rather than as a defence.

**Proposal 11–2** Specific secrecy offences that include extensive codification of permissible disclosure should be reviewed to establish whether these exceptions are necessary in view of the desirability of simplifying secrecy offences.

**Proposal 11–3** Specific secrecy offences that apply to Commonwealth officers should generally be accompanied by a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.

**Proposal 11–4** In order to ensure consistency, secrecy offence provisions should not specify:

- (a) fines for individuals and corporations different from those that would apply if the formulas set out in the *Crimes Act 1914* (Cth) were adopted;
- (b) penalties different from those that would apply if the alternate penalties for proceeding summarily on an indictable offence set out in the *Crimes Act* were adopted; or
- (c) a penalty punishable on summary conviction when, under the *Crimes Act*, an offence carrying that maximum penalty would otherwise be tried before a jury on indictment.

**Proposal 11–5** The penalties for specific secrecy offences should be reviewed for consistency with the general secrecy offence and the subsequent disclosure offence (Proposals 9–3 to 9–5), and in accordance with Proposals 11–7 to 11–11.

**Proposal 11–6** The maximum penalties for the initial and subsequent unauthorised handling of Commonwealth information under specific secrecy offences should generally be the same, subject to relevant differences in relation to fault elements or the reasonable likelihood of harm.

**Proposal 11–7** Guidance on benchmark penalties for specific secrecy offences, consistent with Proposals 11–8 to 11–11, should be incorporated into the Attorney-General’s Department’s *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*.

**Proposal 11–8** Subject to Proposals 11–9 and 11–10, specific secrecy offences should generally provide for a maximum penalty of two years imprisonment, or a pecuniary penalty not exceeding 120 penalty units, or both.

**Proposal 11–9** Specific secrecy offences should generally provide that, where a person knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:

- (a) have a substantial adverse effect on personal privacy; or
- (b) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation,

the penalty should be a maximum of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both.

**Proposal 11–10** Specific secrecy offences should generally provide that, where a person knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:

- (a) harm the national security, defence or international relations of the Commonwealth;
- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
- (c) endanger the life or physical safety of any person; or
- (d) pose a serious threat to public health or public safety

the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.

**Proposal 11–11** Specific secrecy offences that provide for maximum penalties of imprisonment for less than six months, or by pecuniary penalties only, should be reviewed and considered for repeal.

## 12. Specific Secrecy Offences: Simplification and Consistency

**Proposal 12–1** Commonwealth secrecy offences should generally be:

- (a) repealed where the scope of the offences substantially replicates the proposed general secrecy offence; and
- (b) retained where the offences differ in significant and necessary ways from the proposed general secrecy offence.

**Proposal 12–2** Section 79 of the *Crimes Act 1914* (Cth) should be repealed and a new provision inserted in the *Criminal Code* (Cth) making it an offence for a person, without lawful authority and intending to prejudice the Commonwealth's security or defence, to:

- (a) disclose or obtain information concerning the Commonwealth's security or defence; or
- (b) fail to comply with a direction given by a lawful authority with respect to the use of information concerning the Commonwealth's security or defence.

The offence should be punishable by a maximum penalty of ten years imprisonment and a fine of 600 penalty units.

**Proposal 12–3** The Australian Government should review Commonwealth secrecy offences that are retained with a view to consolidation, where possible, into:

- (a) a single provision or part where multiple secrecy provisions exist in the same Act;
- (b) one Act where multiple secrecy provisions exist in more than one Act for which the same Australian Government agency is, or agencies are, responsible.

**Proposal 12–4** The Australian Government should review Commonwealth secrecy offences that are retained for consistency with the proposed general secrecy offence, in accordance with Proposals 10–1 to 10–8, 11–1 to 11–11, 12–1 and 12–3.

**Proposal 12–5** The Attorney-General's Department should incorporate guidance in the *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* dealing with:

- (a) the circumstances in which the enactment of a specific secrecy offence may be justified;
- (b) the drafting of secrecy provisions so that specific secrecy provisions are consistent with, and do not replicate the scope of, the general secrecy offence.

This guidance should incorporate the drafting advice contained in Proposals 10–1 to 10–8, 11–1 to 11–11, 12–1 and 12–3.

### **13. Administrative Obligations in the Australian Public Service**

**Proposal 13–1** Regulation 2.1 of the *Public Service Regulations 1999* (Cth) should be amended to apply to information:

- (a) to which an Australian Public Service employee has access by reason of his or her employment; and
- (b) where the disclosure is reasonably likely to prejudice the effective working of government.

**Proposal 13–2** Regulation 2.1 of the *Public Service Regulations 1999* (Cth) should specify that, in determining whether a disclosure of information is reasonably likely to prejudice the effective working of government, the disciplinary authority should have regard to factors such as:

- (a) the nature of the information disclosed, including the likelihood that it would be subject to release under the *Freedom of Information Act 1982* (Cth) or through some other means; and
- (b) the circumstances in which the disclosure is made, including whether the Australian Public Service employee took reasonable steps to comply with the agency's information-handling policy or any lawful and reasonable direction concerning the disclosure of information.

**Proposal 13–3** The express prohibition on the disclosure of information communicated in confidence set out in reg 2.1(4) of the *Public Service Regulations 1999* (Cth) should be removed.

**Proposal 13–4** Regulation 2.1 of the *Public Service Regulations 1999* (Cth) should include a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.

**Proposal 13–5** The information-handling policies developed by Australian Government agencies in accordance with Proposal 15–1 should clearly set out the disciplinary penalties that could result from breach of secrecy obligations, including the factors that will be considered in determining any such penalty.

**Proposal 13–6** The *Public Service Act 1999* (Cth) should provide that evidence of information given or documents produced by an Australian Public Service employee

for the purpose of administrative disciplinary proceedings with respect to secrecy obligations is not admissible in criminal proceedings against the employee for the same, or substantially the same, conduct.

## **14. Regulating Beyond the *Public Service Act***

**Proposal 14–1** Australian Government agencies that employ persons other than under the *Public Service Act 1999* (Cth)—including agencies prescribed under the *Financial Management and Accountability Act 1997* (Cth) and bodies subject to the *Commonwealth Authorities and Companies Act 1997* (Cth)—should:

- (a) include in the agency’s terms and conditions of employment the requirements set out in reg 2.1 of the *Public Service Regulations 1999* (Cth), to the extent that these requirements are consistent with the agency’s functions and structure; and
- (b) adopt the safeguards set out in the *Public Service Act* for dealing with suspected breaches of reg 2.1, to the extent that these safeguards are consistent with the agency’s functions and structure.

**Proposal 14–2** Australian Government agencies should remind employees, on termination, of their continuing liability under the general secrecy offence and any relevant specific secrecy offence, and of their obligations under the equitable duty of confidence.

**Proposal 14–3** An Australian Government agency that enters into a contract for services involving access to Commonwealth information should include in the contract a confidentiality clause that:

- (a) clearly sets out the categories of information that are confidential Commonwealth information;
- (b) requires persons (other than Commonwealth employees) who have access to confidential Commonwealth information by reason of the contract to agree to comply with the contractual confidentiality requirements; and
- (c) permits the disclosure of confidential Commonwealth information where the disclosure amounts to a public interest disclosure under proposed Commonwealth public interest disclosure legislation.

**Proposal 14–4** The Australian Government should include in the terms and conditions of appointment for members of boards and committees:

- (a) secrecy requirements equivalent to those imposed on Commonwealth employees in a related employment context, to the extent that these requirements are consistent with the board’s or committee’s function and structure; and

- (b) the right to terminate the appointment of a member in the event of a breach of the secrecy obligation.

**Question 14–1** Are there any situations in which neither administrative penalties nor contractual remedies apply to an unauthorised disclosure of Commonwealth information? If so, are civil penalties a suitable way to address these gaps in application or are there other, better ways of dealing with these situations?

**Proposal 14–5** Australian Government agencies should review administrative secrecy requirements that differ from the revised reg 2.1 of the *Public Service Regulations 1999* (Cth), including ‘lawful and reasonable directions’ issued to employees to ensure that these are consistent with the implied constitutional freedom of political communication.

## 15. Fostering Effective Information-Handling Practices

**Proposal 15–1** Australian Government agencies should develop and implement policies clarifying the application of relevant secrecy laws to their information holdings. These policies should include:

- (a) the types of information that an employee can lawfully disclose in the performance of his or her duties;
- (b) the types of information for which an employee must obtain authority for disclosure, including the potential for unauthorised disclosure to result in disciplinary action;
- (c) the circumstances in which the unauthorised handling of information could lead to criminal proceedings; and
- (d) avenues for an employee to raise queries or concerns, including the process by which he or she can make a public interest disclosure.

**Proposal 15–2** Australian Government agencies should make their information-handling policies publicly available, save in certain exceptional cases where this would be unreasonable or impractical.

**Proposal 15–3** Australian Government agencies that regularly share information with other agencies or bodies should enter into memorandums of understanding setting out the terms and conditions for the exchange of information.

**Proposal 15–4** Australian Government agencies should develop and administer training and development programs for their employees, on induction and at regular intervals thereafter, about the information-handling obligations relevant to their

position, including the circumstances in which it is appropriate to share information and the avenues for making public interest disclosures.

**Proposal 15–5** Any Australian Government agency that administers oaths, affirmations or declarations of secrecy should ensure that these properly reflect what is required under relevant Commonwealth secrecy laws.

**Proposal 15–6** Australian Government agencies should put in place and maintain information and communication technology systems to facilitate the secure and convenient handling of Commonwealth information, including access controls and audit mechanisms.

**Proposal 15–7** Private sector organisations that perform services for or on behalf of the Australian Government under contract should take steps to ensure that all employees who access Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal, civil or administrative liability could result.

# 1. Introduction to the Inquiry

---

## Contents

Background	23
Recommendations for a review	24
A plethora of provisions	27
Scope of the Inquiry	29
Terms of Reference	29
Definitions	29
Mapping secrecy laws	32
Matters outside this Inquiry	33
Process of reform	34
Timeframe for the Inquiry	34
Advisory Committee	35
Issues Paper 34	35
Inquiry Snapshot	36
Community consultation	36
Written submissions	38
Discussion Paper 74	38
Overview	38
Chapter structure	39

## Background

1.1 On 5 August 2008, the Attorney-General of Australia, the Hon Robert McClelland MP, asked the Australian Law Reform Commission (ALRC) to conduct an Inquiry into options for ensuring a consistent approach across government to the protection of Commonwealth information, balanced against the need to maintain an open and accountable government through providing appropriate access to information. The Terms of Reference, which are set out at the front of this Discussion Paper, are headed ‘Review of Secrecy Laws’.

1.2 ‘Secrecy laws’ are collectively those provisions that protect Commonwealth information by imposing obligations on those who handle it. The most general of such provisions is s 70 of the *Crimes Act 1914* (Cth):

- (1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he or she is authorized to publish or communicate it, any fact or document which comes to his or her knowledge, or into his or her

possession, by virtue of being a Commonwealth officer, and which it is his or her duty not to disclose, shall be guilty of an offence.

(2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him or her), any fact or document which came to his or her knowledge, or into his or her possession, by virtue of having been a Commonwealth officer, and which, at the time when he or she ceased to be a Commonwealth officer, it was his or her duty not to disclose, shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

1.3 Section 70 has been described as ‘a pretty wide provision’.<sup>1</sup> It is also not alone in imposing obligations on Commonwealth officers with respect to the handling of information. In the course of the Inquiry to date the ALRC has identified 507 provisions that can be described as secrecy provisions, 358 of which create secrecy offences.

### **Recommendations for a review**

1.4 In its report supporting the introduction of the *Freedom of Information Act 1982* (Cth) (FOI Act), the Senate Standing Committee on Legal and Constitutional Affairs urged the Australian Government to reconsider s 70, as it was ‘implausible to enact a presumption of openness while leaving untouched provisions like section 70 that provide the legal foundation for the system of discretionary secrecy that presently exists’.<sup>2</sup> The Committee also noted that many secrecy provisions conflicted diametrically with the philosophy espoused in the Freedom of Information Bill 1978 (Cth).<sup>3</sup>

1.5 Commonwealth secrecy laws have been considered in a number of other reviews and inquiries, either directly or indirectly. In 1983, the Human Rights Commission reviewed the *Crimes Act* and found that s 70 could operate in a manner inconsistent with art 19 of the *International Covenant on Civil and Political Rights* (freedom of expression). The Commission recommended that s 70 be amended to limit its operation to the kinds of information in respect of which restrictions may be imposed under art 19.3—these being for the protection of national security or public order, or of public health or morals.<sup>4</sup>

---

1 Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 269 (P Glynn).

2 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 1979* (1979), [21.24].

3 Ibid, 236.

4 Human Rights Commission, *Review of the Crimes Act 1914 and Other Crimes Legislation of the Commonwealth* (1983).

1.6 In 1991, a committee chaired by Sir Harry Gibbs undertook a review of Commonwealth criminal law (Gibbs Committee),<sup>5</sup> including secrecy provisions that imposed criminal sanctions. The Committee concluded that:

It is undesirable that the sanctions and machinery of the criminal law should be applied in relation to the unauthorised disclosure of all forms of official information and this should be avoided if possible.<sup>6</sup>

1.7 The Gibbs Committee recommended that s 70 of the *Crimes Act* as well as s 79—which deals with the unauthorised communication of official secrets—should be repealed, and that

the application of criminal sanctions under the general criminal law of the Commonwealth to disclosure of official information should be limited to certain categories of information and that these should be no more widely stated than is strictly required for the effective functioning of Government.<sup>7</sup>

1.8 The Gibbs Committee went on to consider what categories of information should be protected by criminal sanctions. These included information relating to intelligence and security services, defence or foreign relations, and information obtained in confidence from other governments or international organisations.<sup>8</sup>

1.9 In 1994, the Senate Select Committee on Public Interest Whistleblowing recommended that the existing provisions of the *Crimes Act* be amended to allow the disclosure of information in the public interest to be a defence against prosecution.<sup>9</sup>

1.10 In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs again considered the operation of ss 70 and 79 and noted the longstanding calls for reform.<sup>10</sup> The Committee identified a number of problems with the sections. These included the lack of precision in the drafting—particularly since the duty not to disclose referred to in s 70 is not located in the *Crimes Act* itself—and the application of the sections to officers not employed under the *Public Service Act 1922* (Cth).<sup>11</sup> The Committee also noted the lack of consistency in drafting and penalties across the secrecy provisions in other Commonwealth statutes.<sup>12</sup> The Committee recommended that the existing secrecy provisions should be rationalised and consolidated into a general offence within the *Crimes Act*.<sup>13</sup>

---

5 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991).

6 Ibid, 315.

7 Ibid, 317.

8 Ibid, 317–321.

9 Australian Parliament—Senate Select Committee on Public Interest Whistleblowing, *In the Public Interest* (1994), [9.53].

10 Australian Parliament—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), 90–91.

11 Ibid, 91–92.

12 Ibid, 95.

13 Ibid, 118.

1.11 Protection for whistleblowers again became the focus of attention in the release in February 2009 of the report of the House of Representatives Standing Committee on Legal and Constitutional Affairs (House of Representatives Standing Committee), *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector*, which recommended that a Public Interest Disclosure Bill be introduced to Parliament as a matter of priority.<sup>14</sup> As explained by the Chair of the Committee, Mark Dreyfus QC MP, the recommendations in the report

reflect what the Committee considers to be primary legislative priorities. They promote integrity in public administration and support open and accountable government. They are informed by the view that legislation should be based on clear commonsense principles to provide reasonable certainty to any person reading it. Yet legislation alone is not sufficient. A shift in culture needs to take place to foster a more open public sector that is receptive to those who question the way things are done.<sup>15</sup>

1.12 The principal focus of the recommendations of the House of Representatives Standing Committee is to protect a broad range of employees in the public sector, as well as contractors and consultants, who make public interest disclosures and may be subject to secrecy provisions. The Committee recommended that whistleblower protection provide immunity from criminal liability (including under secrecy offences).<sup>16</sup>

1.13 The ALRC itself has had occasion to comment on secrecy laws in three prior reviews. First, in 1995, the ALRC and the Administrative Review Council recommended that a thorough review of all Commonwealth legislative provisions prohibiting disclosure of government-held information by public servants be conducted to ensure that such provisions did not prevent the disclosure of information that was not exempt under the FOI Act.<sup>17</sup>

1.14 Secondly, in 2004, in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC recommended that:

The Australian Government should review all legislative and regulatory provisions giving rise to a duty not to disclose official information—including in particular regulation 2.1 of the *Public Service Regulations*—to ensure the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.<sup>18</sup>

---

14 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 1.

15 Ibid, ix.

16 Ibid, Rec 14.

17 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 13.

18 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

1.15 Thirdly, in 2008, in *For Your Information: Australian Privacy Law and Practice* (ALRC 108), the ALRC recommended that:

The Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.<sup>19</sup>

1.16 All the recommendations for a review of secrecy laws were prompted in large measure by the great number and diverse range of secrecy provisions.

### A plethora of provisions

1.17 In the Terms of Reference the Attorney-General listed, as the first matter to which he had regard,

the desirability of having comprehensive, consistent and workable laws and practices in relation to the protection of Commonwealth information.<sup>20</sup>

1.18 As noted above, the ALRC has identified 507 secrecy provisions. They have been introduced at different times, in different language and often with widely ranging penalties. John McGinness has noted that:

With the expansion of the Commonwealth's role after the mid-1940s in areas such as taxation, health, education, welfare, scientific research, industry assistance and regulation, secrecy provisions increased in number as a reflection of the increase in personal and commercially sensitive information collected by the government.<sup>21</sup>

1.19 The lack of consistency among the many provisions was remarked upon in 1991 by Professor Paul Finn:

When one amalgamates the plethora of statutory provisions, regulations, codes, administrative instructions and common law rules one is left in almost every Australian jurisdiction with an ill-fitting, sometimes unintelligible mosaic of prescriptions and proscriptions. For the individual official the consequence of this can be conflicting, sometimes quite unacceptable, legal demands: the trivial can be criminalised, the important left in a state of lamentable uncertainty.<sup>22</sup>

1.20 There are several intertwined issues in Finn's observations that provide a relevant backdrop to this Inquiry and the desire to achieve comprehensive, consistent and workable laws. First, a basic practical matter was to identify the 'plethora' of provisions—without that work 'it's a wilderness', it was remarked in an early consultation.<sup>23</sup> The map that has been produced by the ALRC—described below—

---

19 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 15–2.

20 The Terms of Reference are set out at the front of this Discussion Paper.

21 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 49.

22 P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 92.

23 New South Wales Bar Association, *Consultation SC 08*, Sydney, 8 October 2008.

provides a thorough picture of all relevant provisions and a basis for comparison and analysis throughout the Inquiry.<sup>24</sup>

1.21 Secondly, a key challenge is to identify the core principles or values underpinning the ‘mosaic of prescriptions and proscriptions’ noted by Finn<sup>25</sup> and to distinguish these from the values in play in relation to other Commonwealth provisions concerning information.

1.22 Information handling, management and protection in the Commonwealth context can be expressed as a spectrum, or continuum. At the ‘open government’ end of the spectrum, we find information that should be disclosed as a matter of course. It is now common practice for most Commonwealth departments and agencies to maintain websites that provide an enormous amount of information. This is both desirable, in the interests of promoting open and accountable government in a democratic society, as well as practical and efficient—the more information that is readily available to the public in this way, the fewer requests, questions and FOI applications there are departmental officers to have to handle. Then there is the information that is available through the mechanism of a request under the FOI Act. This also includes information that is not normally available to the public—for example, where it is covered by an exception to FOI disclosure rules, but nevertheless may be disclosed in the exercise of discretion by a departmental head or other senior officer. Moving towards the ‘protected information’ end, one finds information that is shared through specific agreement, protocols or legislative arrangements amongst government agencies and with private sector partners, but is otherwise protected through confidentiality and secrecy provisions. Finally, there is the information that is strictly secret and closely protected—most obviously, information relating to national security or ongoing law enforcement operations, but also many other categories of information that are exempt from FOI legislation. Even at this end of the spectrum, however, there may be circumstances in which information that is otherwise secret can be revealed through prescribed ‘public interest disclosure’ (or ‘whistleblower’) mechanisms.

1.23 Thirdly, the consequences of the provisions for the individual officer need to be examined closely so that the penalty regime is an appropriate fit for that which is restricted or proscribed; and the individual is not left in a state of ‘lamentable uncertainty’<sup>26</sup> with respect to their conduct in relation to Commonwealth information. Aspects of this problem were identified in ALRC 98 where it was also recommended that, in conducting the review of secrecy provisions, a clear distinction should be drawn between conduct that gives rise to administrative sanctions and conduct that gives rise to criminal sanctions.

---

24 Appendix 4 lists all criminal and non-criminal provisions identified by the ALRC to date.

25 P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 92.

26 Ibid.

## Scope of the Inquiry

### Terms of Reference

1.24 The Terms of Reference are reproduced at the beginning of this Discussion Paper. The ALRC is directed to focus on options for ensuring a consistent approach across government to the protection of Commonwealth information as well as providing appropriate access to information in the interests of maintaining an open and accountable government.

1.25 During the course of the Inquiry the ALRC is directed to consider:

- a. relevant laws and practices relating to the protection of Commonwealth information, including the scope and appropriateness of legislative provisions regarding secrecy and confidentiality;
- b. whether there is a need to consolidate and modernise relevant provisions currently in the *Crimes Act 1914* (Cth) and other Commonwealth legislation for inclusion in the *Criminal Code* (Cth);
- c. the way in which secrecy laws in the *Crimes Act* interact with other laws and practices, including those relating to secrecy, privacy, freedom of information, archiving, whistle-blowing, and data-matching;
- d. whether there should be different considerations for secrecy laws relating to the protection of national security and other sensitive Commonwealth information; and
- e. any related matter.

### Definitions

1.26 This Inquiry concerns ‘secrecy laws’ in relation to ‘Commonwealth information’, often in the hands of a Commonwealth officer. Each expression requires some definition.

#### *Secrecy laws*

1.27 A key preliminary step in this Inquiry is to identify what provisions are included in the concept of secrecy provisions, as there is no established definition of the term ‘secrecy law’ or ‘secrecy provision’.

1.28 Commonwealth secrecy provisions and the information they protect are varied. There are offences of general application, like s 70 of the *Crimes Act*, that prohibit disclosure of *any* information a government officer has obtained in their official capacity that he or she has a duty not to disclose. Other provisions are quite specific, and prohibit the disclosure of identified classified, sensitive or personal information.

1.29 In reviewing the range of provisions that should be considered in this Inquiry, the ALRC has identified, for example, provisions that deal with communicating or disclosing information; provisions about receiving information that is secret; and those concerning misuse of information. Issues of secrecy are also aspects of the

management of information in an administrative sense, as well as being the subject of specific prescription in legislation.

1.30 For the purposes of this Inquiry, the ALRC has adopted a broad approach to the characterisation of secrecy provisions and defined a secrecy provision as a provision in an Act or subordinate legislation that imposes secrecy or confidentiality obligations.

1.31 Secrecy provisions are not limited to restricting disclosure of information. They may cover a chain of conduct that leads to possible disclosure—such as soliciting, obtaining, copying, using, retaining, divulging, and communicating information. They also may include provisions dealing with receipt of disclosed information. All the provisions identified, however, are focused on protecting the confidentiality of the information.

1.32 There are related provisions that sit outside this definition, as their principal focus is not the protection of information through obligations of confidentiality or secrecy. These have not been included in the concept of ‘secrecy law’ for the purpose of this Inquiry. Examples include provisions that:

- prohibit the misuse of information for personal gain—as the principal concern of such provisions is fraud, not protection of the confidentiality of the information;<sup>27</sup>
- concern the storage, modifying or destroying of information; and
- permit the disclosure of, for example, personal information in certain circumstances—as the core aim concerns privacy of personal information.

1.33 Aspects of practice and procedure regarding the protection of information and management of information handling are also relevant and are considered separately in Chapter 15.

### ***Commonwealth information***

1.34 ‘Commonwealth information’ (which may also be called ‘government information’) is information developed, received or collected by or on behalf of the Commonwealth government. It includes information the Commonwealth receives from individuals (such as personal information provided to an agency like Centrelink),

---

27 This was a matter that was referred to in the review of Commonwealth criminal provisions in 1991: H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991). In Part V, ‘The Disclosure of Official Information’, after a consideration of existing Australian law regarding disclosure of official information, comparative law and options for reform, a chapter was included concerning ‘Misuse of Official Information for Private Gain’: ch 33. The Committee considered that such a matter could be included, if at all, under other provisions of the *Crimes Act* or a proposed new offence. It was, therefore, peripheral to what were considered secrecy provisions in the report.

information developed in-house (for example, intelligence reports) and information generated by foreign governments that is shared with the Commonwealth government.

1.35 Commonwealth information may be classified into a number of categories based upon their ‘sensitivity’. The *Australian Government Protective Security Manual* (PSM)<sup>28</sup> binds all Commonwealth agencies to a series of procedures designed to protect Commonwealth information, including classified information and other sensitive information. The PSM also refers to ‘official information’, which includes any information received or collected by, or on behalf of, the government, through its agencies and contractors.<sup>29</sup>

1.36 Once information is classified, it is marked accordingly and given various forms of protection—including restricting access to people with a security clearance at the appropriate level; physical protection, such as storage in approved containers of sufficient strength or meeting other security standards; and restrictions on how it may be transferred from one person to another. Chapter 15 discusses in detail the PSM and other manuals, policies and guidelines relating to information handling to which Commonwealth officers (and other persons made privy to Commonwealth information) are subject. The protection of classified and security sensitive information was also considered in ALRC 98.<sup>30</sup>

1.37 Outside the classification process, documents prepared for use by the Commonwealth Cabinet to formulate policy and make decisions are given special protection on the basis that unauthorised disclosure would damage the fullness and frankness of discussions in the Cabinet Room and would thereby inhibit the process of good government. These documents are marked Cabinet-in-Confidence regardless of any other security considerations. The Cabinet Handbook stipulates that Cabinet-in-Confidence documents require a level of protection at least equivalent to that given to documents classified as ‘Protected’ under the guidelines set out in the PSM.<sup>31</sup>

1.38 However, the fact that information is neither classified nor a Cabinet document does not mean that it is freely available. Other legislation or the common law duty of confidence may also protect Commonwealth information in certain circumstances; and although the FOI Act gives the public rights of access to government-held or government-controlled information, this is subject to a number of exceptions and exemptions.<sup>32</sup>

28 Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM) [Summary]* (2006) <<http://www.ag.gov.au>> at 15 October 2008.

29 Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM)* (2005), pt C, [1.3].

30 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004). See also Ch 3.

31 Australian Government Department of the Prime Minister and Cabinet, *Cabinet Handbook* (5th ed, 2004), [7.5].

32 See Ch 4.

***Commonwealth officer***

1.39 Individuals who may be subject to secrecy obligations in relation to Commonwealth information are sometimes referred to as Commonwealth officers and sometimes as public service employees or similar terms.

1.40 The *Crimes Act* includes a general prohibition against the unauthorised disclosure of official information by current and former Commonwealth officers.<sup>33</sup> ‘Commonwealth officers’ are defined as including those appointed or engaged under the *Public Service Act 1999* (Cth), those holding office under, or employed by, the Commonwealth, and those who perform services by or on behalf of the Commonwealth.<sup>34</sup>

1.41 The *Public Service Act* refers to Australian Public Service (APS) employees, and includes those employed in Australian Government departments and statutory agencies. ‘Commonwealth officer’, defined in the *Crimes Act*, includes, but is wider than, ‘APS employees’. These definitions are discussed in more detail in Chapter 8.

1.42 For the purposes of this Inquiry, the wider expression is used unless the context requires a narrower term.

***Whistleblower***

1.43 The term ‘whistleblower’ is of relatively recent origin. The Macquarie Dictionary suggests that the term emerged in the United States in the second half of the 1960s from the phrase ‘blow the whistle on’. It is now commonly used even in official contexts, as, for example, the House of Representatives Standing Committee’s report, referred to above,<sup>35</sup> and in s 16 of the *Public Service Act*.

1.44 In this Inquiry, the term ‘whistleblower’ is used to refer to someone who makes a public interest disclosure, for example, alleging that the conduct of a Commonwealth officer or agency is corrupt or involves maladministration. This topic is discussed in greater detail in Chapter 9.

**Mapping secrecy laws**

1.45 As part of the background research work for this Inquiry, the ALRC undertook a ‘mapping exercise’ to identify and analyse secrecy provisions. As noted above, for the purposes of this Inquiry, the ALRC has defined secrecy provisions broadly as any provision in primary or subordinate legislation that imposes secrecy or confidentiality obligations.

---

33     *Crimes Act 1914* (Cth) s 70.

34     Ibid s 3.

35     Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

1.46 The 507 secrecy provisions identified by the ALRC are scattered throughout 175 pieces of primary and subordinate legislation. These provisions are listed in a table in Appendix 4. Approximately 70% of the statutory secrecy provisions identified expressly impose criminal penalties for breach of secrecy or confidentiality obligations. These provisions are listed in the first section of the table in Appendix 4. The remaining provisions set out a duty of secrecy or confidentiality or establish rules for the handling of protected information and may provide for civil or administrative penalties for breach of such duties. These provisions are listed in the second section of the table in Appendix 4. While such provisions do not in themselves create an offence, s 70 of the *Crimes Act* may operate to attach criminal sanctions to the breach by a Commonwealth officer of these provisions.

1.47 The table does not include provisions that merely clarify or inform the operation of a secrecy provision, such as exception provisions that set out the circumstances in which the handling of Commonwealth information will not breach a secrecy provision.

1.48 The ALRC has used this map of secrecy laws as a basis for comparing and analysing the scope of current secrecy laws and to inform the development of proposed reforms. Figures drawn from the data are expressed throughout this Discussion Paper in approximate percentage values, usually rounded to the nearest 5%. Percentage values will differ according to whether the assessment includes all secrecy provisions or only offence provisions.

### Matters outside this Inquiry

1.49 In reviewing Commonwealth secrecy provisions, the Terms of Reference ask the ALRC to consider ‘relevant laws and practices relating to the protection of Commonwealth information’. The idea of protecting Commonwealth information can be conceived broadly. It can encompass issues as varied as how files and documents are physically protected; whether the classification processes are appropriate and effective; or the extent to which the production of Commonwealth information can be compelled from Commonwealth officers in the course of investigations or in legal proceedings. It could also encompass other rules of evidence under which certain information cannot be adduced in courts or tribunals.

1.50 The ALRC’s approach in this Inquiry is informed by the emphasis in the Terms of Reference on the increased need to share information ‘within and between governments and with the private sector’—namely, the business of government, rather than the business of courts and tribunals. In addition, the ALRC has addressed the use of government information in courts and tribunals to some extent in a prior report.

1.51 In ALRC 98, the ALRC considered the protection of classified and security sensitive information in the context of court and tribunal proceedings.<sup>36</sup> The ALRC recommended the introduction of a new National Security Information Procedures Act, which would apply to all Australian courts and tribunals. Many of these recommendations were implemented by the enactment of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

1.52 In this Inquiry the ALRC considers both the scope and appropriateness of current secrecy provisions and how they affect the ability of information to flow between agencies, governments, and with the private and community sectors, to complement prior recommendations.<sup>37</sup>

1.53 The focus of the Inquiry is therefore on provisions concerning the secrecy and confidentiality obligations of individual Commonwealth officers (or other people nominated in legislation) and the information they acquire by virtue of their position. Review of the government's larger security and information management systems is outside the scope of this Inquiry.

## **Process of reform**

### **Timeline for the Inquiry**

1.54 The timeframe for the Inquiry is set by the Terms of Reference and the necessity to embark upon a thorough and staged process of consultation.

1.55 The ALRC's standard practice is to produce an Issues Paper and a Discussion Paper, prior to producing the final Report. Both the Issues Paper and the Discussion Paper may be obtained free of charge in hard copy or on CD from the ALRC or may be downloaded free of charge from the ALRC's website <[www.alrc.gov.au](http://www.alrc.gov.au)>.

1.56 The Report, containing the final recommendations, is due to be presented to the Attorney-General by 31 October 2009 for tabling<sup>38</sup> in the Australian Parliament, at which point the Report becomes a public document.<sup>39</sup>

1.57 ALRC Reports are not self-executing documents. The ALRC is an advisory body and provides recommendations about the best way to proceed, but implementation is always a matter for Government and others.<sup>39</sup>

---

36 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004).

37 Ibid; Australian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [15.158].

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

39 However, the ALRC has a strong record of having its advice followed. About 58% of the ALRC's previous reports have been fully or substantially implemented, about 29% of reports have been partially implemented, 8% of reports are under consideration and 5% have had no implementation to date: Australian Law Reform Commission, *Annual Report 2007–08*, ALRC 109 (2008), 42.

## Advisory Committee

1.58 A key aspect of ALRC procedures is to establish an expert Advisory Committee or ‘reference group’ to assist with the development of its inquiries.<sup>40</sup> In this Inquiry, the Advisory Committee includes judges, heads and senior officers of Australian Government agencies, academics, senior lawyers, and an FOI consultant.

1.59 The Advisory Committee has particular value in helping the ALRC to identify the key issues and determine priorities, providing quality assurance in the research, writing and consultation processes. The Advisory Committee will also assist with the development of proposals and recommendations for reform as the Inquiry progresses. Ultimate responsibility for the Report and recommendations, however, remains with the Commissioners of the ALRC.

1.60 The Advisory Committee met for the first time on 30 October 2008, to consider the questions to be included in the Issues Paper. It met for the second time on 19 March 2009, to consider the proposals contained in this Discussion Paper. A third (and final) meeting will be held before the completion of the final Report, to consider the draft recommendations for reform.

## Issues Paper 34

1.61 *Review of Secrecy Laws*, ALRC Issues Paper 34 (IP 34) was released electronically on 9 December 2008 and on 17 December 2008 in hard copy format, in order to commence the community consultation process on an informed basis.

1.62 Divided into seven chapters, IP 34 was intended to identify the main issues relevant to the Inquiry, provide background information, and encourage informed community participation by stimulating full and open discussion of the issues arising from the Terms of Reference.

1.63 IP 34 set out 65 questions that the ALRC identified as arising out of the Terms of Reference and which required comment before the ALRC could formulate the proposals for reform contained in this Discussion Paper.

1.64 To date, the ALRC has received 45 written submissions. Lists of the submissions are set out in Appendix 1. Two submissions were made as confidential submissions and one contained a confidential appendix.

1.65 Submissions were received, for example, from: government law enforcement and investigative bodies—including the Australian Federal Police, the Commonwealth Director of Public Prosecutions and the Australian Intelligence Community; government agencies—such as the Department of Human Services, the Australian

---

40 A list of Advisory Committee members can be found in the List of Participants at the front of this Discussion Paper.

Taxation Office and the Treasury; tribunals and oversight bodies—including the Commonwealth Ombudsman and the Social Security Appeals Tribunal; lawyers—both through the representative group, the Law Council of Australia, and by individuals; media groups—such as Australia’s Right to Know coalition and the Australian Press Council; lobby groups—such as Fairness in Child Support and Whistleblowers Australia; and individuals.

1.66 With the release of this Discussion Paper, the ALRC once again invites individuals and organisations to make submissions to the Inquiry prior to the release of the final Report.

### **Inquiry Snapshot**

1.67 To facilitate communication about the nature and focus of this Inquiry the ALRC released an overview document, *Review of Secrecy Laws—Inquiry Snapshot*, in February 2009. It is written in plain language and provides a ready access to information about the Inquiry and is available online as a virtual document. Like other ALRC publications, it can be downloaded free from the ALRC website: <[www.alrc.gov.au](http://www.alrc.gov.au)>.

### **Community consultation**

1.68 The Terms of Reference indicate that the ALRC ‘is to identify and consult with key stakeholders, including relevant Commonwealth, State and Territory agencies and private sector bodies’.

1.69 One of the most important features of ALRC inquiries is the commitment to widespread community consultation.<sup>41</sup> The nature and extent of this engagement is normally determined by the subject matter of the reference—particularly whether the topic is regarded as a technical one, of interest largely to specialists in the field, or is a matter of interest and concern to the broader community. Some ALRC inquiries—such as those relating to children and the law, Aboriginal customary law, multiculturalism and the law, the protection of human genetic information, and privacy—have involved a significant level of interest and involvement from the general public and the media. Others, like the inquiry into client legal privilege and federal investigations, were of particular interest to legal practitioners and Commonwealth agencies.

1.70 The ALRC is based in Sydney but, in recognition of the national character of the body, consultations are conducted around Australia during the Inquiry. Any individual or organisation with an interest in meeting with the Inquiry in relation to the matters raised in this Discussion Paper is encouraged to contact the ALRC.

---

41 B Opeskin, ‘Measuring Success’ in B Opeskin and D Weisbrod (eds), *The Promise of Law Reform* (2005) 202.

1.71 To date, consultations have been held with a number of government agencies, Commonwealth public servants, academics, judges and members of the legal profession. A full list of consultations is set out in Appendix 2.

1.72 Under the provisions of the *Australian Law Reform Commission Act 1996* (Cth), 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.<sup>42</sup> In this regard the ALRC is utilising two additional strategies for consultation in this Inquiry—an online forum and a national phone-in. A phone-in was undertaken during the Privacy Inquiry and proved a valuable means of obtaining personal experiences, insights, ideas and concerns that complemented the other forms of consultation through submissions and face-to-face meetings.<sup>43</sup>

1.73 The phone-in for this Inquiry was conducted on 11 and 12 February 2009. The ALRC received thirty-four calls over the two-day period. The concerns expressed included matters such as: inappropriate revelations of personal information or perceived breaches of privacy; difficulties of gaining access to personal information for the purpose, for example, of family reunion; problems with security classifications—overclassification—and obtaining security clearances; cultures of secrecy in agencies and a desire to keep problems ‘in house’; problems of obtaining information under the FOI Act; the need for whistleblower protection; difficulties in the sharing of information amongst agencies; and the draconian nature of s 70 of the *Crimes Act*.

1.74 To facilitate public communication in relation to the Inquiry, the ALRC also initiated a ‘Talking Secrecy’ online forum, again following upon the success of the ‘Talking Privacy’ website established in connection with the Privacy Inquiry.<sup>44</sup> The ‘Talking Secrecy’ online forum takes this a step further as an interactive site, or ‘blog’. The object of such websites is to create a ‘talking space’ in relation to each ALRC inquiry, to provide information about the inquiry in an accessible manner.

1.75 After moderation, the ALRC posted 12 contributions to the online forum. Comments included matters about agency culture; the security classification system under the PSM; the application of tax secrecy provisions to information about public companies; internet censorship proposals; the need for, and problems in devising, effective information and risk management systems; and who should be subject to secrecy obligations.

1.76 The questions on the ‘Talking Secrecy’ online forum will be changed to reflect the proposals in this Discussion Paper and to seek further comment in addition to the process for making written submissions.

---

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

43     The ‘National Privacy Phone-in’ is described in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [1.89]–[1.91].

44     Ibid, [1.92]–[1.93].

### **Written submissions**

1.77 With the release of this Discussion Paper, the ALRC invites individuals and organisations to make submissions in response to the specific proposals, or to any of the background material and analysis provided, to help advance the reform process in this Inquiry.

1.78 There is no specified format for submissions and they may be marked confidential if preferred. The ALRC will gratefully accept anything from handwritten notes to detailed commentary and scholarly analyses on Commonwealth secrecy laws. Although not essential, the ALRC prefers electronic communications and submission may be made simply by contributing comments online at the ALRC's website—even simple dot-points are welcome.

1.79 The ALRC appreciates that the tight deadline for making submissions—both in response to the Issues Paper and this Discussion Paper—places considerable pressure upon those who wish to participate in the Inquiry. The ALRC acknowledges the considerable amount of work undertaken by those who have contributed to the consultative processes to date. Given the deadline for delivering the final Report to the Attorney-General, and the need to consider fully the submissions received in response to this Discussion Paper, all submissions must be submitted on time—by Friday 7 August 2009.

1.80 It is the invaluable work of participants that enriches the whole consultative process of ALRC inquiries. The quality of the outcomes is assisted greatly by the understanding of contributors in needing to meet the deadline imposed by the reporting process itself. This Inquiry is no exception.

## **Discussion Paper 74**

### **Overview**

1.81 This Discussion Paper contains a more detailed treatment of the issues raised in the Issues Paper and indicates the Inquiry's current thinking in the form of specific reform proposals.

1.82 The focus of the proposals is to provide a principled basis for a revised general secrecy offence, complemented by criteria for review of specific secrecy provisions and revised administrative procedures and penalty structures aimed at fostering effective information handling in the public sector.

1.83 However, the proposals contained in this Discussion Paper do not represent the final recommendations of the Inquiry. The ALRC is seeking further submissions and is undertaking a further round of national consultations and it is not uncommon for there to be some significant changes of approach between a Discussion Paper and Final Report. If there are passages in this paper that appear to imply that definitive conclusions have already been drawn about the final recommendations, this is

unintended and not meant to inhibit full and open discussion of policy choices before the Inquiry's program of research and consultation is completed.

1.84 In recent times, the ALRC's approach to law reform has involved a mix of strategies including: legislation and subordinate regulations, official standards and codes of practice, industry and professional guidelines, education and training programs, and so on. Proposals—and, later, recommendations—may be directed to the Attorney-General, to whom the Report is presented, and also to other government and non-government agencies, associations and institutions for action or consideration.

1.85 Finally, it should be noted that in the past the ALRC often drafted legislation as the focus of its law reform effort. The ALRC's practice has since changed, and it does not produce draft legislation unless specifically asked to do so in the Terms of Reference for a particular inquiry. This is partly because drafting is a specialised function better left to the parliamentary experts, and partly because 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, but its final recommendations will specify the nature of any desired legislative change.

## **Chapter structure**

1.86 This Discussion Paper is divided into 15 chapters. Proposals for reform are not spread evenly throughout. Some chapters provide mainly contextual or background material, which does not lend itself to specific reform proposals, particularly in the earlier part of the Discussion Paper. Other chapters are more focused on technical aspects of the law and practice—it is in these chapters that the reform proposals are mainly found.

1.87 The chapters fall into four broad areas:

- concepts and comparisons;
- a general criminal secrecy offence;
- specific secrecy offences; and
- administrative duties, practices and procedures.

### ***Concepts and comparisons***

1.88 The first five chapters provide the conceptual framework of secrecy laws, including comparisons with other major Commonwealth legislation and an overview of the confidentiality and secrecy obligations under common law and legislation.

1.89 Chapter 2 provides a consideration of the broad conceptual framework for the Inquiry and the interaction and tension between ideas of secrecy and accountability of

government. It also includes a consideration of the concept of ‘public interest’ in both its general and specific senses, and contrasts approaches to the protection of Commonwealth information, on the one hand focusing on categories of information, on the other, on the harm caused by disclosure.

1.90 Chapter 3 focuses on information sharing by the Australian Government for the purpose of satisfying governmental policies and programs. This will usually involve the sharing of information between Australian Government agencies, but it may also include the sharing of information with state and territory agencies or the private sector. The chapter summarises the various ways in which information is shared, including, for example, through data matching and memorandums of understanding operating within a broad commitment to a ‘whole of government’ response to policy making.

1.91 Chapter 4 considers the relationship between Commonwealth secrecy laws and other Commonwealth laws dealing with the handling of information—in particular, the FOI Act, the *Archives Act 1983* (Cth) and the *Privacy Act 1988* (Cth). It also refers to proposed amendments in each area.

1.92 Chapter 5 provides a broad overview of obligations of secrecy both under the common law and secrecy provisions in Commonwealth legislation. The chapter reviews the number and location of secrecy provisions in Commonwealth legislation today, outlines the different types of information that these provisions are designed to protect and provides an analysis of the elements of secrecy and confidentiality provisions. In particular, this chapter examines questions such as whose activity is regulated by Commonwealth secrecy provisions, and what kind of activity is regulated.

#### *A new general offence*

1.93 Chapter 6 examines the role of administrative, civil and criminal penalty provisions in regulating the disclosure of Commonwealth information, as well as the need for a general secrecy offence. The Chapter proposes that ss 70 and 79(3) of the *Crimes Act* should be repealed and replaced by a new general secrecy offence in the *Criminal Code* in which the prosecution should be required to prove that a particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to specified public interests, such as the security or defence of the Commonwealth.

1.94 The following three chapters focus on different aspects of the proposed general secrecy offence. Chapter 7 considers the kinds of public interest that should be protected by a general secrecy offence. Chapter 8 considers some of the essential elements of the proposed new offence—including whose conduct, and what kind of conduct, should be regulated. Chapter 9 considers what exceptions and defences should be available under the proposed general secrecy offence, and what penalties should apply for breach.

***Specific secrecy offences***

1.95 Chapters 10, 11 and 12 review specific secrecy offences—that is, secrecy offences other than ss 70 and 79(3) of the *Crimes Act*, which have general application to Commonwealth officers and information—in the light of the proposed general secrecy offence and the policy basis for that offence. The aim of this process is to develop proposals to promote consistency in, and simplification of, Commonwealth secrecy offences.

1.96 Chapter 10 discusses how specific secrecy offences should be framed in order to be more consistent with the general secrecy offence, and with each other, and highlights aspects of the general secrecy offence that might usefully be more broadly adopted. The key elements of the offences considered in this chapter are: requirements for a reasonable likelihood of harm; the relevant conduct; fault elements; the parties to offences; and the nature of the information protected. Chapter 11 repeats this approach with respect to exceptions and defences, and penalties.

1.97 Chapter 12 examines the criteria involved in assessing whether there is substantial replication and identifies examples of offences that, subject to more detailed review, might be repealed on this basis. The chapter also discusses general concerns about lack of consistency in the drafting of specific secrecy offences and ways to address this problem, including through the consolidation of existing secrecy offences. The chapter also suggests a process for implementing reform and develops proposals to ensure that this process is informed by the ALRC's conclusions, primarily through the development of detailed drafting directions and other guidance against which existing and proposed new secrecy offence provisions can be evaluated.

***Administrative duties, practices and procedures***

1.98 The final three chapters focus on the administrative secrecy framework in the Australian Government.

1.99 Chapter 13 considers the administrative secrecy obligations of persons engaged as Australian Public Service (APS) employees under the *Public Service Act 1999* (Cth), and makes a number of proposals for clarifying and consolidating these obligations. Procedural safeguards for the investigation and enforcement of administrative secrecy obligations are also discussed.

1.100 Chapter 14 proposes models for harmonising the administrative secrecy regimes that apply to Commonwealth employees other than APS employees—such as members of the Australian Defence Force, members of the Australian Federal Police and employees of public authorities—with the *Public Service Act* framework. The chapter also considers mechanisms for regulating persons that are not in an ongoing employment relationship with the Australian Government, such as private sector contractors and former Commonwealth employees.

1.101 Chapter 15 discusses the extent to which the above strategies contribute to the compliance of Commonwealth officers with secrecy laws and other information-handling obligations, and makes suggestions for possible improvements. The chapter goes on to consider information handling at the level of Australian Government agencies, in particular, the role of independent oversight bodies in fostering an effective information-handling culture at the agency level. Finally, the chapter considers information handling in the private sector.

In order to ensure consideration for use in the final Report, submissions addressing the proposals in this Discussion Paper must reach the ALRC by **Friday, 7 August 2009**. Details about how to make a submission are set out at the front of this publication.

## **2. Open Government, Secrecy and Public Interest**

---

### **Contents**

Introduction	43
Why secrecy?	44
Towards openness	46
The idea of accountability	48
Background	48
Scrutiny of government actions	49
Balancing secrecy laws with accountability	51
Submissions	53
ALRC's views	58
Secrecy laws and the Australian Constitution	58
The implied freedom of political communication	59
Separation of powers	66
The public interest	71
Background	71
A wide concept	72
A unifying thread	73
Contrasting approaches	75
ALRC's views	77

### **Introduction**

2.1 In reviewing Commonwealth secrecy laws in this Inquiry, the Australian Law Reform Commission (ALRC) has been asked to have regard to the importance of balancing, on the one hand, the need to protect Commonwealth information and, on the other, the public interest in an open and accountable system of government. This raises the issue of when the balance of ‘public interests’ requires Commonwealth information to be protected rather than being freely available on the premise of open and accountable government.

2.2 Both values—secrecy and openness—reflect certain historical understandings of the relationship between a government, its citizens, its officials and information. One fundamental component in that relationship is the interaction between secrecy laws and the *Australian Constitution*, including the implied freedom of political communication and the separation of powers.

2.3 However, at the heart of the challenge of balancing secrecy with openness lies the question of ‘why secrecy?’ at all, as well as what is the meaning, or meanings, of ‘public interest’. In setting the scene for a consideration of the proper role and function of secrecy provisions in Commonwealth laws today, this chapter will explore some of the key ideas in the conceptual landscape.

## Why secrecy?

2.4 For most of Australia’s history, ‘official secrecy has been the legislatively enforced norm’.<sup>1</sup> The first secrecy provision was introduced in the colony of Victoria in 1867<sup>2</sup> and it ‘set the pattern for the various public services of Australia’.<sup>3</sup> It provided that:

no information out of the strict course of official duty shall be given directly or indirectly, by any officer without the express direction or permission of the responsible Minister.<sup>4</sup>

2.5 The idea that secrecy of official information was necessary is based on the ‘Westminster system’ of government, inherited from the United Kingdom.<sup>5</sup> An essentially closed system, it is based upon ministerial responsibility, in which secrecy in relation to the mechanisms of advising ministers—such as Cabinet deliberations and documents—is critical. It is also complemented by the view of the public servant as neutral and anonymous and precluded from public comment on government actions or policies.<sup>6</sup> As explained by the Independent Review Panel examining the Queensland *Freedom of Information Act 1992*, chaired by David Solomon (Solomon Committee):

Secrecy had been an essential ingredient of the system—secrecy to protect the deliberations of the cabinet, secrecy to protect the advice proffered by public servants to their ministers, secrecy to hide what happened within the public service. The democratic element that allowed this closed system to function was provided by the concept of ministerial responsibility—ministers were responsible, collectively and individually, directly to parliament and indirectly to the electorate, for what the government did, and for what their departments did.<sup>7</sup>

2.6 The idea that government information is a special commodity is a much older one, however. As Professor Enid Campbell has explained, the notion that the activities of government should be secret goes back to a period where monarchs were motivated

<sup>1</sup> P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 90.

<sup>2</sup> Ibid, 89.

<sup>3</sup> Ibid.

<sup>4</sup> This provision was found in reg 20 of the 1867 Regulations for Victoria’s *Civil Service Act 1862*: Ibid, 9.

<sup>5</sup> G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 34–35.

<sup>6</sup> 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), Ch 4.

<sup>7</sup> Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), 158.

by a desire to protect themselves against their rivals and official information was considered the property of the Crown, to be disclosed or withheld at will.<sup>8</sup>

2.7 In contrast, in the United States (US), government information is relatively more accessible.<sup>9</sup> In Sweden a great deal of personal information about individuals is made available online by government<sup>10</sup>—quite different from the position in the UK, US and Australia which have legislative regimes that, to varying degrees, restrict disclosure of information about individuals.<sup>11</sup>

2.8 In Australia, the perceived need to protect official information is reflected in the first Commonwealth secrecy provisions, passed during the initial session of the Australian Parliament in 1901 and aimed at protecting national security information.<sup>12</sup> But as the reach of government expanded, so too did secrecy provisions. As John McGinness notes,

with the expansion of the Commonwealth's role after the mid-1940s in areas such as taxation, health, education, welfare, scientific research, industry assistance and regulation, secrecy provisions increased in number as a reflection of the increase in personal and commercially sensitive information collected by the government.<sup>13</sup>

2.9 Periods of international conflict have precipitated an awareness of the need for, and experience of, secrecy provisions. For example, World War II and the Cold War ‘provided a setting where secrecy was linked to military strength’.<sup>14</sup> Moreover, many senior ministers in the 1950s and 1960s had served in World War II, and had been ‘imbued with the military’s respect for secrecy’.<sup>15</sup> In 1960, amendments were made to s 70 of the *Crimes Act 1914* (Cth),<sup>16</sup> inspired in part by the anti-communist climate of

8 E Campbell, ‘Public Access to Government Documents’ (1976) 41 *Australian Law Journal* 73, 77.

9 In the US, legislation establishing rights of access to government records in limited circumstances was enacted in 1946, and legislation establishing a general right of access was enacted in 1966: *Administrative Procedure Act of 1946* 60 Stat 237 (US) and *Freedom of Information Act of 1966* 80 Stat 383 (US). See J Michael, ‘Freedom of Information in the United States of America’ in N Marsh (ed) *Access to Government-Held Information* (1987) 55.

10 The first Swedish Act that provided for rights of access to government documents was enacted in the mid-18<sup>th</sup> century: *Freedom of Press Act 1766* (Sweden). See also G Petren, ‘Access to Government-Held Information in Sweden’ in N Marsh (ed) *Access to Government-Held Information* (1987) 35. The *Personal Data Act 1998* (Sweden) regulates the processing of data about individuals, but a significant number of Swedish government records are published online: E Addley, ‘Sweden Tries to Lose Reputation as Snoopers’ Paradise’, *Guardian Unlimited Technology* (online), 19 June 2007, <technology.guardian.co.uk>.

11 See *Data Protection Act 1998* (UK), *Privacy Act of 1974* 5 USC § 552a ; *Privacy Act 1988* (Cth).

12 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 49. These provisions were ss 9 and 127 of the *Post and Telegraph Act 1901* (Cth).

13 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 49.

14 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 41.

15 Ibid.

16 Section 70 of the *Crimes Act 1914* (Cth) is a general secrecy provision which is discussed throughout this Discussion Paper, especially in Ch 6. It is set out in full in Appendix 3.

the Cold War,<sup>17</sup> which had the effect of strengthening the provision by extending the reach of the section to former Commonwealth officers. However, as Greg Terrill notes, s 70 was ‘just one of many secrecy provisions inserted or strengthened in legislation after the war’.<sup>18</sup>

## Towards openness

2.10 The 1960s saw a change in approach to official secrecy with the development of a new philosophical and practical approach to government known as ‘open government’.<sup>19</sup> As Terrill notes:

The logic was simple. As government became more a part of their lives, so people outside government needed or wished to know more about these influences, and to affect decisions.<sup>20</sup>

2.11 Freedom of information—FOI—laws were the response. Following the introduction of such legislation in the US, a number of speeches, papers and editorials in the late 1960s and early 1970s raised the profile of the concept of FOI in Australia and propelled the inclusion of legislation on the parliamentary agenda.<sup>21</sup>

2.12 In 1970, the then Leader of the Opposition, the Hon Gough Whitlam MP, stated that ‘it is clear that after 20 years in government excessive secrecy has become commonplace in governmental decision making’.<sup>22</sup> Introduction of FOI legislation became an issue prior to the 1972 federal election,<sup>23</sup> at which time the Australian Labor Party claimed that the government’s monopoly of knowledge had ‘led to bad decisions and bad government’.<sup>24</sup>

2.13 During the early 1970s, a number of government committees were set up federally and in some of the Australian states to examine the review of administrative decisions in light of the growing impetus towards openness—particularly influenced by developments in this regard in the US and in contrast to the adherence to a more closed

---

17 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 45.

18 Ibid.

19 Freedom of Information Review Panel, *Enhancing Open and Accountable Government*, Discussion Paper (2008), 158.

20 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 43.

21 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [3.2].

22 Commonwealth, *Parliamentary Debates*, House of Representatives, 20 May 1970, 2428 (G Whitlam—Leader of the Opposition), cited in G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), I, 14.

23 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [3.2]; G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 15.

24 G Whitlam, *It's Time for Leadership: Policy Speech for the Australian Labor Party delivered at the Blacktown Civic Centre* (1972) <<http://www.australianpolitics.com/elections/1972>> at 23 October 2008.

system of government in the UK. The introduction of FOI legislation remained a key political issue during the 1970s.<sup>25</sup>

2.14 The legislative reforms that eventually followed became known as the ‘new administrative law’, the purpose of which was to facilitate effective public administration while at the same time safeguarding the civic rights of the individual citizen.<sup>26</sup>

2.15 The initial package of legislation included the *Ombudsman Act 1976* (Cth), the *Administrative Appeals Tribunal Act 1975* (Cth) and the *Administrative Decisions (Judicial Review) Act 1977* (Cth). These Acts established mechanisms for enhancing the accountability of government departments and public servants and ‘together provided a framework for control of government action’.<sup>27</sup> In addition, the Administrative Review Council was set up as part of an integrated system of administrative review, with ongoing responsibility for promoting, educating and advising on administrative law principles, and balancing the provision of justice for the individual citizen against the interests of the Government in implementing the programs and policies for which it was elected.<sup>28</sup>

2.16 The *Freedom of Information Act 1982* (Cth) (FOI Act) was passed in 1982, embracing in a formal way the concept of open government. The FOI Act was followed by the *Archives Act 1983* (Cth), which established a regime for the storage of, and public access to, government records. The enactment of the FOI Act was considered a ‘major step in establishing open government’ and a significant step towards overturning ‘a deeply entrenched tradition of government secrecy’.<sup>29</sup>

2.17 The move away from a closed to a more open system is also evident in the UK—the home of the Westminster system—in its introduction of the *Freedom of Information Act 2000*, which came into force only in January 2005. To assist in

---

25 See, eg, Interdepartmental Committee on Proposed Freedom of Information Legislation, *Proposed Freedom of Information Legislation* (1974) Australian Government Attorney-General’s Department; Interdepartmental Committee on Proposed Freedom of Information Legislation, *Policy Proposals for Freedom of Information Legislation: Report of Interdepartmental Committee* (1976) Australian Government Attorney-General’s Department; 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).

26 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), 3–4.

27 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).

28 The Administrative Review Council (ARC) was established under pt V of the *Administrative Appeals Tribunal Act 1975* (Cth). For information about the ARC see: Administrative Review Council, Home page <<http://www.ag.gov.au/agd/WWW/arcHome.nsf/Page/Home>> at 29 April 2009.

29 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), 3.

preparation for the operation of the Act and to facilitate its implementation once in effect, the Office of Information Commissioner was established. The Office has a dual purpose—to promote access to official information and protect personal information.<sup>30</sup>

2.18 At the same time as access to government information was being opened up, however, the increase in the size and roles of government, combined with technological advances that enhanced the ability of government to deal with large amounts of information, led to concerns about the handling and management of personal information in the hands of public servants. The *Privacy Act 1988* (Cth) was the result, concerning the retention and management of personal information and reflecting a philosophy of protection and individual control of such information.<sup>31</sup>

2.19 Both the FOI Act and the *Privacy Act* contain provisions in relation to personal records and information.<sup>32</sup> The precise interaction of FOI, privacy and secrecy regimes is quite complex and is considered in Chapter 4. The pivotal question is how far the idea of accountability should go? FOI exemptions, secrecy provisions and information-handling practices are just some of the matters that are affected by the response to this question. As a preliminary consideration for the following chapters, the idea of accountability and the place for secrecy provisions in that context will be considered.

## The idea of accountability

### Background

2.20 Access to, and openness of, government information is based on the idea of accountability—that a representative democratic government is open to account for its actions, policies and administrative decisions, a key part of which is public access to the information on which action and policies are based.<sup>33</sup> As Rocque Reynolds has argued:

Governments have access to, and control of, vast amounts of information which may be personal, commercial, sensitive, confidential or politically and socially significant. How governments collect, store, use and disclose this information; whether the public has access to such information; and when governments are required to generate or provide information to the public, tells us a lot about the relationship between the state and its citizens.<sup>34</sup>

---

30 Information Commissioner's Office (UK), *About the ICO* <[http://www.ico.gov.uk/about\\_us.aspx](http://www.ico.gov.uk/about_us.aspx)> at 19 November 2008.

31 In 2000 the *Privacy Act* was amended to include the National Privacy Principles for the private sector: *Privacy Amendment (Private Sector) Act 2000* (Cth).

32 The relationship between the two Acts was a subject of consideration in the ALRC inquiry on privacy: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), ch 15.

33 H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995), 92.

34 R Reynolds, 'Obtaining Reasons for Government Decision-Making, FOI and Privacy' in R Cryke and J McMillan (eds), *Control of Government Action* (2005) , [18.1.1].

2.21 That ‘the public’ now includes an increasing group of ‘Net Geners’—the 12- to 30-year old cohort or ‘Net Generation’—adds a further imperative of openness:

To win the trust of Net Geners, governments have to be transparent ... At a minimum, policy makers should publicize their overall goals and objectives and, for specific issues and decisions, the documents they relied on, the names of the participants in the decision-making process, and their underlying rationales and criteria, and they should provide reasons why alternative policy options have not been pursued.<sup>35</sup>

2.22 In response to the Issues Paper, *Review of Secrecy Laws*<sup>36</sup> (IP 34), Bill Calcutt drew attention to the ‘fundamental challenge in a liberal democracy’ of finding the balance between the rights of individuals and the powers of the state:

Accountability is a vital safeguard against the abuse of power by the state. Accountability ensures justification for the exercise of authority is scrutinized and responsibility attributed. Accountability is central to learning from experience.<sup>37</sup>

2.23 Echoing such sentiments, Whistleblowers Australia expressed the view that:

information in the possession of the public sector should be available for public consumption as a matter of course. This view is soundly based. In our system of representative government it is essential that the functions and activities of the public sector are as transparent as possible. It is a right of Australian citizens to be informed as they wish about matters of public administration.<sup>38</sup>

### Scrutiny of government actions

2.24 In the 1992 report of the Royal Commission into the commercial activities of the Western Australian government, a principal recommendation of which was the introduction of FOI legislation in that state, it was commented that: ‘[i]n a democratic society, effective accountability to the public is the indispensable check to be imposed on those entrusted with public power’.<sup>39</sup>

The purpose of [accountability] measures is to hold governments, public officials and agencies to account for the manner of their stewardship. Government is constitutionally obliged to act in the public interest. To the extent that it is given power to do so, it must be allowed to do so. Such is its trust. Accountability provides the test and measure of its trusteeship.<sup>40</sup>

35 L Crovitz, ‘Can We Trust Anyone Over 30?’ *The Wall Street Journal*, 10 November 2008, <<http://online.wsj.com>>, referring to remarks of Don Tapscott, the ‘best-selling author and researcher’ about the differences for children ‘Growing Up Digital’, as the title of his 1997 publication was called.

36 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

37 B Calcutt, *Submission SR 10*, 11 February 2009.

38 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

39 *Report of the Royal Commission into Commercial Activities of Government and Other Matters* (1992), pt II, [3.1.1].

40 *Ibid*, [3.1.5].

2.25 A principal plank of accountability relies upon access to information to provide public scrutiny of government actions—‘because the public has a *right to know*’:

Openness in government is the indispensable prerequisite to accountability to the public. It is a democratic imperative. The right to vote is without substance unless it is based on adequate information. If government is to be truly government for the people, if the public is to be able to participate in government and to experience its benefits, the public must be properly informed about government and its affairs.<sup>41</sup>

2.26 The ‘right to know’ is the focus of the FOI Act, reflected in its long title: ‘An Act to give to members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies’. It is also expressly stated in s 3(1) that the object of the Act is ‘to extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth’, which is further emphasised in s 3(2):

It is the intention of the Parliament that the provisions of this Act shall be interpreted so as to further the object set out in subsection (1) and that any discretions conferred by this Act shall be exercised as far as possible so as to facilitate and promote, promptly and at the lowest reasonable cost, the disclosure of information.

2.27 The importance of accountability based on access to information was recently reiterated by Senator the Hon John Faulkner, Cabinet Secretary and Special Minister of State, in announcing an Exposure Draft of the Freedom of Information Amendment (Reform) Bill 2009 (FOI Exposure Draft Bill):

The slow growth of the idea that government accountability extends beyond answering to electors on polling day has gradually changed the way Australian governments treat government information. With that has come a recognition that the best safeguard against ill-informed public judgement is not concealment but information. As Abraham Lincoln said: ‘Let the people know the facts, and the country will be safe.’

There is a growing acceptance that the right of the people to know whether a government’s deeds match its words, to know what information the government holds about them, and to know the information that underlies debate and informs decision-making is fundamental to democracy.<sup>42</sup>

2.28 In the Companion Guide to the FOI Exposure Draft Bill, Senator Faulkner emphasised the importance, in this context, of the ‘right to know’:

Both in practice, and as a symbol, ‘freedom of information’ represents the pinnacle of citizens’ right to know: a legal requirement to give the Australian community access to information held by the Australian Government.<sup>43</sup>

---

<sup>41</sup> Ibid, [2.1.3].

<sup>42</sup> J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

<sup>43</sup> J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009) See also J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

2.29 It is also proposed that the objects clause of the FOI Act be revised in line with this emphasis:

- (1) The objects of this Act are to give the Australian community access to information held by the Government of the Commonwealth, by:
  - (a) requiring agencies to publish the information; and
  - (b) providing for a right of access to documents.
- (2) The Parliament intends, by these objects, to promote Australia's representative democracy by contributing towards the following:
  - (a) increasing public participation in Government processes, with a view to promoting better-informed decision-making;
  - (b) increasing scrutiny, discussion, comment and review of the Government's activities.
- (3) The Parliament also intends, by these objects, to increase recognition that information held by the Government is to be managed for public purposes, and is a national resource.
- (4) The Parliament also intends that functions and powers given by this Act are to be performed and exercised, as far as possible, to facilitate and promote public access to information, promptly and at the lowest reasonable cost.<sup>44</sup>

2.30 Complementing the commitment towards revising the FOI Act is the work of the House of Representatives Standing Committee on Legal and Constitutional Affairs (House of Representatives Standing Committee), which released its report, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector*, in February 2009 (the *Whistleblower Protection* report).<sup>45</sup> In recommending protection to a broad range of employees in the public sector as well as contractors and consultants, who may be subject to secrecy provisions, the House of Representatives Standing Committee effectively provides a 'right to reveal' where the matter is regarded as a disclosure in the public interest—in the circumstances and in the manner proposed.

2.31 The challenge, then, is to identify the proper place, if any, for secrecy provisions in the context of a system of open and accountable government.

### Balancing secrecy laws with accountability

2.32 The idea of secrecy conflicts conceptually with the ideas of openness and accountability. From the very outset of the FOI era in Australia, the challenge of

<sup>44</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, s 3 'Objects—general'. The section is complemented by s 3A 'Objects—information and documents otherwise accessible'.

<sup>45</sup> Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

finding the proper role of secrecy provisions was acknowledged. When commenting on the Freedom of Information Bill 1978 (Cth), the Senate Standing Committee on Legal and Constitutional Affairs noted that the philosophy of open government appears to conflict diametrically with that underlying secrecy provisions.<sup>46</sup>

2.33 The Senate Standing Committee also criticised what it then described as ‘a fashionable contemporary drafting practice’:

to insert in every new statute a standard provision making it an offence for an official governed by the statute to disclose without authorisation any information of which he has gained knowledge officially.<sup>47</sup>

2.34 The routine inclusion of secrecy offences in Commonwealth statutes may open up an avenue for criticism, such as that reflected in the submission received from Whistleblowers Australia in response to IP 34:

Secrecy and confidentiality are important tools for the protection of the public interest. But secrecy and confidentiality are also convenient tools used for the manipulation of information to benefit particular people.<sup>48</sup>

2.35 Such a sentiment was echoed by a caller in the ALRC’s secrecy phone-in, who remarked that, while there is a genuine need to protect government issues, the use of secrecy provisions was ‘the second last refuge of the scoundrel’ and that a change in culture, accompanied by appropriate education, were critical.<sup>49</sup>

2.36 In a conference speech on 24 March 2009, at which he announced the release of the FOI Exposure Draft Bill,<sup>50</sup> Senator Faulkner stated that committing to greater openness of government through an amended FOI regime,

has not lifted from Australian governments their responsibilities to safeguard confidentiality, privacy and security. But it has required them to evaluate and define responsibilities in the democratic arena. ...

No government broadcasts the activities of its intelligence services, the contents of sensitive diplomatic negotiations, or the precise location of troops, for example. And no government should. But *our* democracy, drawing as it does so strongly on the heritage of Westminster, has inherited a historical tendency to weight the protective features of confidentiality more heavily than the positive aspects of disclosure.

And ... this has been an underlying tension in the development of Freedom of Information laws in Australia.<sup>51</sup>

---

46 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), 236.

47 Ibid, 233.

48 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

49 *Secrecy Phone-In*, 11–12 February 2009.

50 Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft.

51 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

2.37 Where FOI provisions are directed towards making government information accessible, through obligations of publication and also through applications, secrecy provisions impose obligations of confidentiality on designated people, such as Commonwealth officers. However the conflict between open government—as a philosophy of government—and secrecy as an obligation of working practice for individual public servants may generate uncertainties, as reflected in the following comment:

the individual official—and particularly the public servant—is often enough caught between the present commitment both of modern legislation and of the common law to open government and the enduring demands of illiberal official secrecy regimes.<sup>52</sup>

2.38 In view of such conflict, it is fair to ask: do we need secrecy provisions at all? The sufficiency of common law rules to answer the need for protection of information is considered in Chapter 5. The relevance of secrecy laws in the context of modern accountability commitments expressed, for example, in FOI laws is considered here.

### Submissions

2.39 In IP 34, the ALRC asked whether secrecy laws were still relevant and necessary in the light of FOI laws and other modern moves towards greater openness and accountability on the one hand, and the current international security environment on the other.<sup>53</sup>

2.40 A number of stakeholders strongly supported the principle of access to government documents. For example, the Law Council of Australia commented that:

the principle of open and accountable government, which underpins the FOI Act, is concerned with ensuring Governments, Ministers and other public officials behave appropriately and in accordance with public expectations. This includes allowing the public to scrutinise whether a public or elected official has misused power, misrepresented the truth, maintained false records, made a decision on improper grounds, etc. Further, it allows the public to investigate the basis upon which certain decisions have been made and provides an avenue to access information held by government instrumentalities which will better inform debates about matters of public interest.<sup>54</sup>

2.41 To similar effect, the Media, Entertainment & Arts Alliance, an active partner in the ‘Australia’s Right to Know’ (ARTK) coalition, argued that:

democracy requires accountability and that accountability is best ensured through open government. In its policy document released prior to the 2007 Federal Election, the ALP identified a ‘culture of concealment’ which had grown up within the government and public service and promised to ‘drive a cultural shift across the

---

52 P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 94.

53 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 1–1.

54 Law Council of Australia, *Submission SR 30*, 27 February 2009.

bureaucracy to promote a pro-disclosure culture'. The Alliance supports this objective which we believe to be greatly in the public interest. ...

In one of his first pronouncements on being elected President of the United States of America, Barack Obama called for the development, by executive departments and agencies, of an Open Government Directive, to promote transparent, collaborative and participatory government under his administration. At the heart of that commitment is the presumption in favour of disclosure, recognising that 'in the face of doubt, openness prevails'. The Alliance believes that the Australian public deserve no less a commitment from our own elected officials.<sup>55</sup>

2.42 However, stakeholders also recognised the need to protect government information in some circumstances. Bill Calcutt acknowledged that at times—'in exceptional circumstances'—'the community may choose to temporarily compromise individual rights and empower the state to act preemptively', but stressed the importance of 'the community' in being able to subject state actions to scrutiny in the interests of accountability.<sup>56</sup>

2.43 The differences in views centred upon those circumstances that justified protection, and the extent of it—in particular the role and nature of secrecy obligations on Commonwealth officers and others. The ARTK coalition argued that access to and sharing of government information is 'an essential right' of every Australian and 'fundamental to openness, transparency and accountability in government'. It was strongly opposed to secrecy provisions as 'an anathema to that right', except where 'public interest' required them:

Any approach to the question of secrecy should be that public access should only be excluded if it is in the public interest. More narrow and restrictive political or bureaucratic considerations that persist in much of the current legislation should not be relevant considerations.

The law in its current form is far too focussed on the rights of government and the bureaucracy and places too little emphasis on the fundamental proposition that access to information should be allowed.<sup>57</sup>

2.44 While the Australian Government Attorney-General's Department (AGD) acknowledged that '[o]penness and accountability are very important principles in a modern democracy', it also emphasised that secrecy provisions 'have a place in modern government because there is still a public interest in certain information being protected from general disclosure'.<sup>58</sup>

---

55 Media Entertainment & Arts Alliance, *Submission SR 39*, 10 March 2009.

56 B Calcutt, *Submission SR 10*, 11 February 2009.

57 Australia's Right to Know, *Submission SR 35*, 6 March 2009. But, as the ARTK coalition also noted, 'Defining what is caught within the ambit of the term "government information" is a threshold step in ensuring there are appropriate parameters around secrecy laws'.

58 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

2.45 That ‘public interests’ are protected by secrecy provisions was also highlighted by the Australian Securities and Investments Commission (ASIC):

ASIC receives, collects and develops information of a varied nature in the course of performing its functions and exercising its powers. A high proportion of that information is received and developed in confidence and could, if disclosed without authorisation, have a material prejudicial effect on both public and private interests. Public interests that may be affected include, at a broader level, the effective functioning of the Australian economy. At a narrower level they include the effective functioning of ASIC. For example, certain disclosures may prejudice the conduct of investigations by ASIC. Other disclosures could inhibit the frankness of communications with government on issues of policy development and law reform that are required to address gaps in regulation. They could also prejudice the receipt of information from foreign regulators.

The disclosure of information could also have a materially adverse effect on a wide variety of private rights and interests.<sup>59</sup>

2.46 ASIC emphasised that, because of the sensitivity of the information that it receives, persons may be ‘less forthcoming’ in providing the information if it were not protected from disclosure.<sup>60</sup> While general law obligations were useful, they were not ‘without uncertainty’.

ASIC believes that, given the significance and materiality of the issue of disclosure, there should be certainty in relation to the scope of confidentiality obligations that apply to Commonwealth bodies and the persons who perform services for them. That certainty would best be achieved by the operation of a statutory duty on Commonwealth officers not to disclose confidential information.<sup>61</sup>

2.47 A number of agencies highlighted the importance of secrecy provisions with respect to their particular operations. For example, the Australian Bureau of Statistics (ABS) considers that secrecy laws are necessary and appropriate to maintain the integrity and quality of the statistics that the ABS produces:

High quality statistical information is fundamental to effective government. Assuring the secrecy of information provided to the ABS is essential to establishing its quality. The secrecy provisions of the *Census and Statistics Act 1905* enable the ABS to make this assurance.<sup>62</sup>

2.48 The argument is made that there is an ‘unwritten compact’ between the ABS and census respondents of guaranteed confidentiality and that this is underwritten by explicit secrecy provisions in the governing legislation. Without this guarantee, the collection of national statistics by the ABS would eventually be compromised.<sup>63</sup>

---

59 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

60 Ibid.

61 Ibid.

62 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

63 Ibid.

2.49 Other federal bodies also emphasised the importance of secrecy provisions in areas that deal with personal information—in particular, the Australian Treasury, the Australian Taxation Office (ATO) and the Department of Education, Employment and Workplace Relations (DEEWR).<sup>64</sup>

2.50 The ATO stressed that it was ‘fundamental’ to the administration of taxation laws ‘that all information concerning the affairs of a particular taxpayer is protected by a tax secrecy provision’.<sup>65</sup> The expectation of the community in relation to the handling of personal information, reinforced by an offence provision, was also emphasised by DEEWR:

there is a level of community expectation that information held by the Department will be protected from not only the unauthorised disclosure of that information but also the inappropriate collection and use of that information. It is generally recognised that the harm that can be caused to the interests of an individual or the Commonwealth from the inappropriate disclosure of information held by the Department can be significant. Because of this, there is a recognised need for there to be consequences flowing from such inappropriate action. ... [H]aving a criminal offence provision which attaches to the unauthorised handling of information has value in being a useful deterrent.<sup>66</sup>

2.51 Secrecy provisions in such contexts, moreover, were not seen to be in conflict with the principle of open and accountable government. In this regard, the Treasury submitted that taxation secrecy provisions were ‘not inconsistent’ with measures ‘designed to increase the openness and transparency of government’:

Taxation secrecy provisions are not designed to hide or conceal the deliberations of government in relation to decisions that can have a significant impact on the affairs of individual taxpayers. Instead they give effect to a legitimate expectation of Australia’s taxpayers that the often sensitive information that they are required to provide to satisfy their taxation obligations will be subject to an appropriate level of protection.<sup>67</sup>

2.52 The ATO made a similar distinction between principles of openness of government and the rationale of taxation secrecy provisions:

Given that taxation secrecy provisions only apply to protect taxpayer information, the ATO considers that they are entirely consistent with the important principles of openness and accountability which are embodied by freedom of information laws. Freedom of information mechanisms assist to ensure government transparency and accountability, however, they are designed to provide access to information about government rather than allow access to sensitive taxpayer information concerning individuals, corporations and other entities.<sup>68</sup>

---

<sup>64</sup> Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009.

<sup>65</sup> Australian Taxation Office, *Submission SR 13*, 16 February 2009.

<sup>66</sup> Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

<sup>67</sup> The Treasury, *Submission SR 22*, 19 February 2009.

<sup>68</sup> Australian Taxation Office, *Submission SR 13*, 16 February 2009.

2.53 The Department of Human Services drew attention to the broad role that secrecy provisions uniquely fulfil:

Secrecy laws ... serve a number of functions not fully realised in reliance on other laws ... They ensure individuals who handle sensitive information have a clear sense of personal responsibility for the protection of that information, not just Australian Public Service employees; they support public confidence in the appropriate management of private information; they provide practical acknowledgement that some information in the possession of the government is more inherently sensitive, and therefore worthy of greater protection, than other information; and they provide a legitimate basis for agencies to refuse to disclose information in appropriate circumstances, and to recover sensitive information inappropriately disclosed. While other legal mechanisms achieve these outcomes to a greater or lesser extent, they are generally not as targeted and direct as secrecy laws can be.<sup>69</sup>

2.54 Information in the hands of intelligence agencies was also seen to require specific protection through secrecy provisions. The Australian Intelligence Community (AIC) submitted that:

Secrecy laws themselves are essential to the effective operation of Australia's intelligence agencies; these agencies would not be able to operate effectively if secrecy laws were repealed or significantly diminished. A statutory duty on Commonwealth officers not to disclose information is fundamental to the operation of AIC agencies.<sup>70</sup>

2.55 The Australian Transaction Reports and Analysis Centre (AUSTRAC) expressed similar concerns and reiterated the necessity and relevance of secrecy provisions to prevent the unnecessary disclosure of information that

- may not be in the public interest or which might be harmful to individuals or
- relates to persons that are the subject of reports to the AUSTRAC CEO under the [*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)] and the [*Financial Transactions Reports Act 1988* (Cth)], or who are reporting entities or dealers under those Acts.<sup>71</sup>

2.56 AUSTRAC's particular areas of concern were national security, law enforcement operations, revenue and/or international relations, where disclosure of AUSTRAC information may affect the:

- ability of Australian Government and State or Territory Government agencies to identify, investigate, apprehend or prosecute suspected offenders;
- safety and anonymity of persons in witness protection, and under-cover operatives;

---

69 Department of Human Services, *Submission SR 26*, 20 February 2009.

70 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

71 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

- safety of employees of reporting entities who provide reports to AUSTRAC, especially in relation to the provision of suspicious matter reports and/or suspect transaction reports;
- integrity of the financial system, including institutional reputation;
- competitive neutrality of reporting entities and cash dealers if commercially sensitive information relating to those entities were to be disclosed; and
- international relations with overseas [Financial Intelligence Units (FIUs)] and foreign governments if information obtained in confidence from these FIUs were to be disclosed.<sup>72</sup>

2.57 Some stakeholders cited other reasons for needing secrecy provisions, such as the ability to ensure that commercially sensitive information is protected. For example, the Department of Climate Change submitted that:

In particular circumstances, it is both necessary and desirable to impose a statutory obligation on Commonwealth officers not to disclose information. In the case of the *[National Greenhouse and Energy Reporting Act 2007 (Cth) Act]*, this is necessary to ensure that commercially sensitive information reported under the Act by corporations is protected, and to ensure confidence in the integrity of the reporting system.<sup>73</sup>

### **ALRC's views**

2.58 The ALRC's view is that there is a case for secrecy provisions, provided that they are clear, consistent and fair, and directed at protecting important public interests. In Chapter 5, the ALRC considers the interrelationship of secrecy provisions and the common law and concludes that there is still a justified place for secrecy provisions in Commonwealth law.

2.59 The problems identified throughout this Inquiry to date have been in relation to the range of secrecy provisions and the lack of clarity for an individual who is subject to them. The proposals articulated in this Discussion Paper are aimed at providing a redrafted general secrecy offence complemented by a balanced framework for an assessment of current provisions as well as a redrafted administrative provision.

### **Secrecy laws and the Australian Constitution**

2.60 In unravelling conflicts between ideas of accountability and ideas of secrecy, a key goal—as suggested in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98)—is to ensure that secrecy provisions are drafted and interpreted consistently with the *Australian Constitution*,<sup>74</sup> in particular the implied constitutional guarantee of freedom of political communication and principles relating to the separation of powers.

---

72 Ibid.

73 Department of Climate Change, *Submission SR 27*, 23 February 2009.

74 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–5(a).

2.61 The *Australian Constitution* establishes a federal system of government in which powers are distributed between the Commonwealth and the six states. The Constitution contains a list of subjects about which the Australian Parliament may make laws. To be valid, secrecy provisions must be able to withstand scrutiny under the *Australian Constitution* against the identified heads of power.

2.62 A number of provisions in the Constitution could be relied upon to provide the constitutional basis for laws dealing with the confidentiality or secrecy of official government information. Section 52, for example, makes clear that the Australian Parliament has exclusive power to make laws on matters relating to Australian Government public service departments.<sup>75</sup>

2.63 The Australian Parliament also has power to make laws that are incidental to the execution of other powers conferred on it.<sup>76</sup> Thus, while the Parliament has express power to make laws concerning, for example, the federal public service, taxation,<sup>77</sup> defence<sup>78</sup> and the census,<sup>79</sup> it may also make laws that are incidental to these matters. Laws dealing with the confidentiality or secrecy of tax, defence, census or other official information might be construed either as laws relating to the public service, tax, defence or the census, or as incidental to these matters.

2.64 There are, however, a number of constitutional requirements that may limit the power of the Australian Parliament to legislate in this area, including the implied constitutional guarantee of freedom of communication about government and political matters. Principles relating to the separation of the powers and functions of the three branches of government—the legislature, executive and judiciary—also affect the application of secrecy provisions to the parliament and judiciary. In particular, the doctrines of parliamentary privilege and the separation of judicial power affect the manner in which Commonwealth secrecy laws are drafted and interpreted.

### The implied freedom of political communication

2.65 The High Court jurisprudence in what have been called the ‘free speech cases’,<sup>80</sup> is relevant to an assessment of the validity of secrecy laws. A leading case in the field is the 1997 decision in *Lange v Australian Broadcasting Corporation (Lange)*,<sup>81</sup> in which the Rt Hon David Lange, the then Prime Minister of New Zealand, sued the

75      *Australian Constitution* s 52(ii).

76      Ibid s 51(XXXIX).

77      Ibid s 51(ii).

78      Ibid s 51(vi).

79      Ibid s 51(xi).

80      *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520; *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104; *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211; *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106; *Nationwide News Pty Ltd v Wills* (1992) 177 CLR 1.

81      *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

Australian Broadcasting Corporation (ABC) for defamation on the basis of statements made in the television programme, ‘Four Corners’, broadcast throughout Australia. Lange alleged that the programme conveyed imputations that he was guilty of abuse of public office and was unfit to hold such office. The ABC argued that the matter complained of was, among other things, published pursuant to a freedom guaranteed by the *Australian Constitution* to publish material in the course of discussion of government and political matters.

2.66 In accepting the argument of the ABC, the High Court affirmed its earlier decisions<sup>82</sup> that there is an implied freedom in the *Australian Constitution* to publish material discussing government and political matters, and that the common law of defamation ‘must conform to the requirements of the Constitution’.<sup>83</sup> The Court stated, however, that laws could be passed to limit that freedom ‘to satisfy some other legitimate end’,<sup>84</sup> but two questions must be answered for their validity:

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 the fulfilment of which is compatible with the maintenance of the constitutionally prescribed system of representative and responsible government ... If the first question is answered ‘yes’ and the second is answered ‘no’ the law is invalid.<sup>85</sup>

2.67 How do secrecy provisions fare in this context? The question arose for consideration in 2003 in *Bennett v President, Human Rights and Equal Opportunity Commission (Bennett)*.<sup>86</sup> Peter Bennett, a public servant employed in the Australian Customs Service, argued that his implied freedom of political communication was invalidly constrained by former reg 7(13) of the *Public Service Regulations 1999* (Cth) (now repealed), which stated that:

An APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head’s express authority, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge.<sup>87</sup>

2.68 Bennett advocated the establishment of a Single Border Protection Agency and made media comment about the same, which led the Chief Executive Officer of Customs to issue a formal direction to him not to comment to the media ‘about public business or anything of which you have official knowledge’, and to advise that formal action for a breach of the Australian Public Service Code of Conduct could result if he

---

<sup>82</sup> *Theophanous v Herald & Weekly Times Ltd* (1994) 182 CLR 104; *Stephens v West Australian Newspapers Ltd* (1994) 182 CLR 211.

<sup>83</sup> *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 556.

<sup>84</sup> *Ibid*, 562.

<sup>85</sup> *Ibid*, 567–568.

<sup>86</sup> *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

<sup>87</sup> *Public Service Regulations 1999* (Cth) reg 7(13), now repealed and replaced by reg 2.1, considered in detail in Ch 13.

did not comply.<sup>88</sup> Bennett considered that his statements were made in his capacity as the President of the Customs Officers Association and argued that he was being threatened unlawfully because of his union activities. An interview with Bennett on radio about proposed cuts to Customs waterfront officers led to action under reg 7(13) and a penalty of salary reduction being imposed.

2.69 After his challenge in the Human Rights and Equal Opportunity Commission (HREOC) was unsuccessful,<sup>89</sup> Bennett sought a review under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) and directly challenged the constitutional validity of the regulation itself. The matter came before Finn J of the Federal Court in 2003.

2.70 First, Finn J gave a detailed historical analysis of the ‘family of provisions’ represented by reg 7(13), remarking that two features of the regulation were ‘immediately arresting’:

The first, reflecting the provenance of the provision, is the archaic character of its terminology. The second is the amplitude of the information coverage it seeks to secure. The only limitations on the information that is caught by the regulation are that the information be ‘about public business’ or that it be ‘anything of which the employee has official knowledge’.<sup>90</sup>

2.71 Secondly, Finn J assessed the regulation against the two-pronged test established in *Lange*, set out above. He held that the first limb of this test was satisfied, in that the regulation controlled the disclosure by public servants of information about the ‘public business’ of the Australian Government. In relation to the second limb, Finn J identified a range of public interests or ‘legitimate ends’ that would be compatible with maintaining the Australian system of representative and responsible government. These legitimate ends included national security, cabinet confidentiality and the maintenance of an impartial and effective public service. They may also include the ‘efficient operation of Government’—a formulation put forward by the Commonwealth in the case—or the ‘effective working of Government’—a formulation put forward in the review of Commonwealth criminal law by the committee chaired by Sir Harry Gibbs (the Gibbs Committee) in 1991.<sup>91</sup>

2.72 Finn J commented on the ‘apparently draconian character’ of reg 7(13) and the possibility that the provision had the potential to produce unreasonable results.<sup>92</sup> The

---

88 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [12]. The APS Code of Conduct is considered in Chapter 13.

89 The HREOC challenge is detailed in *Bennett* at [30]–[42].

90 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [63].

91 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.3].

92 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [64].

particular regulation, was not, therefore, reasonably and appropriately adapted to the legitimate ends identified, being intended to be a ‘catch-all’ provision:

the only limitations on the information that is caught by the regulation are that information be ‘about public business’ or that it be ‘anything of which the employee has official knowledge’. The former of these limitations would seem to encompass all and any aspect of the structure, conduct and operations of public administration ... The reference to ‘official knowledge’ in the alternative limitation refers to the capacity in which information is derived. If it is derived by a person in his or her official capacity it is caught by the regulation ... Neither of the two limitations is, as such, concerned with whether the information in question was or was not otherwise publicly available, or with whether it ought to be or could be made so. Nor are they concerned with whether in a given instance any public interest consideration could reasonably justify a prohibition on disclosure.<sup>93</sup>

2.73 Finn J found, accordingly, that reg 7(13) was inconsistent with the implied freedom of political communication in the *Australian Constitution* as explained in *Lange* and declared it to be invalid. He stated that:

Official secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not. It is unnecessary to enlarge upon why I consider the regulation to be an inefficient provision other than to comment that its ambit is such that even the most scrupulous public servant would find it imposes ‘an almost impossible demand’ in domestic, social and work related settings ...

The dimensions of the control it imposes impedes quite unreasonably the possible flow of information to the community—information which, without possibly prejudicing the interests of the Commonwealth, could only serve to enlarge the public’s knowledge and understanding of the operation, practices and policies of executive government.<sup>94</sup>

2.74 Finn J noted that the state might legitimately seek to regulate or prohibit the disclosure of some official information for reasons of public interest relating to the nature of the information, the circumstances of its generation or acquisition, or the timing or possible consequences of its disclosure. He quoted, as an example, a provision of the UK Civil Service Management Code, which provided that civil servants must not, without authority, disclose official information that has been communicated in confidence within the Government or received in confidence from others; or seek to frustrate or influence the policies, decisions or actions of ministers and others by unauthorised, improper or premature disclosures of official information.<sup>95</sup>

2.75 Finn J distinguished regulating the disclosure of particular information for legitimate reasons from a ‘catch-all’ approach, such as that in reg 7(13) that did not differentiate between types of information or the consequences of disclosure.

---

93 Ibid, [63].

94 Ibid, [98]–[99].

95 Minister for the Civil Service (UK), *Civil Service Management Code* <[www.civilservice.gov.uk/iam/codes/csmc/index.asp](http://www.civilservice.gov.uk/iam/codes/csmc/index.asp)> at 17 September 2008, [4.1.3].

2.76 Even before *Bennett* had been decided, the challenge posed by secrecy laws in the context of the implied freedom had been clearly identified. Richard Jolly, for example, argued that because secrecy laws specifically target the communication of information about government, such laws may require particularly close scrutiny in order to be consistent with the implied freedom of political communication.<sup>96</sup> In noting the High Court jurisprudence on this issue, Jolly emphasised the statement by Mason CJ in *Australian Capital Television v Commonwealth* that, in relation to the communication of information or ideas relevant to public affairs,

only a compelling justification will warrant the imposition of a burden on free communication by way of restriction and the restriction must be no more than is reasonably necessary to achieve the protection of the competing public interest that is invoked to justify the burden on communication.<sup>97</sup>

2.77 The importance of ensuring that secrecy provisions are not cast too widely is recognised in the Australian Government's *Legislation Handbook*, which requires that:

The Attorney-General's Department must be consulted at an early stage on the scope of any new secrecy provisions and on changes to existing secrecy provisions. Secrecy provisions in legislation are to be no broader than is required for the purposes for which they are enacted, particularly bearing in mind the policy underlying the *Freedom of Information Act 1982*.<sup>98</sup>

2.78 It is also not surprising that a secrecy provision can attract scrutiny against the backdrop of free speech when such a provision is mooted in Parliament. As noted by the then Attorney-General, the Hon Daryl Williams AM QC MP, in introducing the Criminal Code Amendment (Espionage and Related Offences) Bill 2002:

There has been considerable media attention focused on the perceived impact that the official secrets provisions ... were alleged to have on freedom of speech and on the reporting of government activities.<sup>99</sup>

2.79 Following the decision in *Bennett*, reg 7(13) of the *Public Service Regulations* was repealed and replaced by reg 2.1,<sup>100</sup> which expressly included the formula of

---

96 R Jolly, 'The Implied Freedom of Political Communication and Disclosure of Government Information' (2000) 28 *Federal Law Review* 42, 47.

97 *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, 143. In this case the High Court considered the constitutional validity of provisions in the *Broadcasting Act 1942* (Cth)—pt IIID—that restricted broadcasting in relation to Commonwealth parliamentary elections and referenda, including prohibiting political advertising on behalf of the government during an election period. Broadcasters were also obliged to make available free of charge time for election broadcasts to political parties. The High Court held that pt IIID was wholly invalid on the ground that it infringed the right to freedom of communication on matters relevant to political discussion that was implied in the system of representative government for which the Constitution provided.

98 Department of Prime Minister and Cabinet, *Legislation Handbook* (1999), [6.27].

99 Commonwealth, *Parliamentary Debates*, House of Representatives, 13 March 2002, 1111 (D Williams—Attorney-General).

100 *Public Service Amendment Regulations (No 1) 2006* (Cth). The text of reg 2.1 is set out in Appendix 3.

‘effective working of government’. Would this be enough, however, to survive scrutiny in the context of the implied freedom? The validity of the new regulation was challenged in the ACT Supreme Court case of *R v Goreng Goreng*.<sup>101</sup>

2.80 This case concerned the breach of reg 2.1 by Ms Tjanara Goreng Goreng.<sup>102</sup> Goreng Goreng had disclosed certain information by email to her daughter—a draft of talking points for discussion between Australia and other countries; and to a member of the administration of an Aboriginal community, Mutijulu, where the government was funding a number of initiatives designed to improve the conditions of the Indigenous community—concerning allegations against a key person involved.

2.81 Relying heavily upon the decision of Finn J in *Bennett*, Goreng Goreng sought a stay of the criminal proceedings on the grounds that reg 2.1 was invalid for infringing her implied freedom of political communication. Her counsel argued that the starting point—as reflected in FOI legislation—was now that government information should be available unless a specific prohibition could be identified.<sup>103</sup>

2.82 Refshauge J, of the ACT Supreme Court, did not accept the argument:

While that general approach is undoubtedly, it does not seem to me to assist in the particular issue I have to determine. If one accepts, as I do, and it seems to me, with respect, that Finn J did in *Bennett’s Case*, that government as an employer has a legitimate interest in preventing disclosures that would or might interfere with their effective operations, the question is not that one starts with a preference for disclosure, but rather how does one determine the limits.<sup>104</sup>

2.83 Moreover, the revised regulation was not, in Refshauge J’s view, a ‘catch-all’ provision like its predecessor, which had been struck down by Finn J, but rather a more focused and targeted provision that sought to protect a legitimate government interest—although he noted that ‘the effective working of government’ did give rise to some indeterminacy requiring the exercise of judgment.<sup>105</sup>

2.84 The operation of reg 2.1 is a key issue in this Inquiry, to ensure, as recommended in ALRC 98,

that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.<sup>106</sup>

---

<sup>101</sup> *R v Goreng Goreng* [2008] ACTSC 74.

<sup>102</sup> This breach triggered an action under s 70(1) of the *Crimes Act 1914* (Cth).

<sup>103</sup> *R v Goreng Goreng* [2008] ACTSC 74, [31].

<sup>104</sup> *Ibid*, [34].

<sup>105</sup> *Ibid*, [37].

<sup>106</sup> Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

2.85 The regulation is considered, and proposals for its further revision suggested, in Chapter 13.

### **Submissions**

2.86 In IP 34, the ALRC asked two questions relevant to the implied freedom of political communication: first, whether reg 2.1 of the *Public Service Regulations 1999* (Cth) provided an appropriate model for protecting Commonwealth information; and, secondly, whether there were other secrecy provisions that may be inconsistent with the implied guarantee.<sup>107</sup> Submissions in relation to the first question and proposals for a revised regulation are considered in Chapter 13.

2.87 In relation to the second question, the Public Interest Advocacy Centre (PIAC) and the AIC drew attention to ss 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth)—enacted after the High Court decisions in *Australian Capital Television Pty Ltd v Commonwealth* and *Lange*,<sup>108</sup> but before the decision in *Bennett*. PIAC expressed the view that:

these secrecy provisions bind staff, contractors and others who interact with defence and security agencies not to communicate information prepared by or on behalf of the agencies with which they are involved, connected with or relating to the performance of agency functions. They do not require disclosure to cause, or be likely or intended to cause, any harm to the public interest, and they impose a penalty of imprisonment for up to two years.

So far as they do not turn on the likely effect of disclosure, do not require proof of any intention to harm security or defence interests, and do not allow for any exception in the case of information tending to show that the agency in question has exceeded its lawful authority, PIAC believes that [these sections] are in need of amendment or repeal, and that any sanction they impose should be limited to civil as opposed to criminal liability.<sup>109</sup>

2.88 In contrast, the AIC submitted that:

No concerns about the validity of the provisions were raised in Parliament when the respective bills were passed and to date, the constitutional validity of these sections has not been raised or challenged.<sup>110</sup>

2.89 The Australian Prudential Regulation Authority (APRA) expressed the view that the secrecy provision in s 56 of the *Australian Prudential Regulation Authority Act*

---

107 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Questions 3–8 and 3–9.

108 *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106; *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.

109 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

110 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

1998 (Cth) (APRA Act) is not inconsistent with the implied constitutional guarantee of political communication.<sup>111</sup>

#### ***ALRC's views***

2.90 The concern expressed by PIAC about the absence of a harm element in the provisions identified is one that can be applied to most of the 358 secrecy offences identified in the mapping exercise undertaken in this Inquiry, described in Chapter 1. The main plank of the proposals in this Discussion Paper, discussed in Chapter 6, is a new general secrecy offence, in which harm to essential public interests is a principal feature. Chapter 13 also proposes a reworking of reg 2.1 to link more clearly the administrative secrecy obligations of APS employees to identified public interests. However there are areas that may require a different approach and particular secrecy offences. This is discussed in Chapters 10–12.

#### **Separation of powers**

2.91 The structure of the *Australian Constitution* reflects the principles of the separation of powers, meaning that the three functions of government—the power to make laws, administer laws and decide disputes—are each conferred on three different bodies established by the Constitution—the Parliament, executive and judicature. Secrecy laws primarily regulate the executive, that is, people and organisations that implement and administer the laws made by the Parliament. The extent to which secrecy laws can affect the activities of the Parliament and the judiciary has not been finally determined. This section briefly discusses some limitations on the application of secrecy laws to the Parliament and judiciary.

##### ***Secrecy laws and the separation of judicial power***

2.92 The strict separation of judicial power is a fundamental principle of the *Australian Constitution*. General secrecy provisions should not, therefore, interfere with, or limit, the exercise of federal judicial power by a federal court.

2.93 While the issue has not been conclusively determined, in the case of *Grollo v Palmer*<sup>112</sup> the High Court considered whether a judge could authorise a telecommunications interception warrant, a task that required strict secrecy. The question in the case was whether investing persons who are judges of the Federal Court with the non-judicial power of authorising the issue of warrants (and therefore in a personal, not a judicial, capacity) was incompatible with the exercise of the judicial functions of a federal court.

2.94 A question was raised before the Court whether a judge, acting in a personal capacity in authorising an interception warrant, would be subject to a duty not to disclose information gained by virtue of that position. While the majority decision of

---

111 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

112 *Grollo v Palmer* (1995) 184 CLR 348.

the High Court did not consider the issue, Gummow J was of the view that secrecy provisions in ss 70 and 79 of the *Crimes Act 1914* (Cth) could not affect the exercise of federal judicial functions by a judge:

whether the source of the duty be in a statute ... or the general law, the ambit of the duty stops short of impeding discharge of the higher duty flowing from Ch III of the Constitution.<sup>113</sup>

2.95 What if specific legislative provisions required a court to keep certain information confidential? In *Gypsy Jokers Motorcycle Club Inc v Commissioner of Police (Gypsy Jokers)*,<sup>114</sup> the Court considered Western Australian legislation that prohibited a court disclosing information identified by the Police Commissioner as confidential to any person, including other parties to the proceeding. Information was confidential if its disclosure might prejudice police operations. Then in *K-Generation Pty Ltd v Liquor Licensing Court (K-Generation)*,<sup>115</sup> the High Court considered the validity of South Australian legislation that required a court, on the application of the Police Commissioner, to take steps to maintain the confidentiality of information classified by the Police Commissioner as criminal intelligence.

2.96 In both cases, the High Court held that the legislation did not interfere with a court's integrity, impartiality or independence, because the court retained the power to determine whether information had been correctly classified as criminal intelligence (in *K-Generation*), or whether the disclosure of the information might prejudice the operations of the Commissioner (in *Gypsy Jokers*). In *K-Generation*, French CJ concluded that:

The terms of [the relevant sub-section] do not subject the Licensing Court or the Supreme Court to the direction of the executive or an administrative authority. The subsection does not require them to receive or act upon criminal intelligence classified as such by the Commissioner of Police. It does not deprive the Court of discretion as to how confidentiality is to be maintained. Nor does it mandate a general exclusion in all circumstances of legal representatives from access to the information. [The provision] does not undermine the institutional integrity of either court. It does not render them unfit repositories for the exercise of federal jurisdiction.<sup>116</sup>

2.97 In this way, specific confidentiality provisions that are directed to the operations of a court are similar to claims of public interest immunity and will not necessarily impair a court's independence and impartiality.

---

113 Ibid.

114 *Gypsy Jokers Motorcycle Club Inc v Commissioner of Police* (2008) 234 CLR 532.

115 *K-Generation Pty Ltd v Liquor Licensing Court* (2009) 252 ALR 471.

116 Ibid, [98]–[99].

### ***Secrecy laws and parliamentary privilege***

2.98 In response to IP 34, the ALRC received a submission from the Clerk of the Senate, Mr Harry Evans, drawing the ALRC's attention to the relationship between secrecy provisions and the operation of parliamentary privilege.<sup>117</sup> Evans submitted that:

From time to time executive government officials suggest that statutory secrecy provisions prevent them providing information to either House of the Parliament or its committees and/or render them liable under such provisions for supplying relevant information.<sup>118</sup>

2.99 He suggested further that secrecy provisions 'may also inhibit the provision of information to the Houses and their committees by prospective witnesses without the inhibition becoming known'.<sup>119</sup>

2.100 'Parliamentary privilege' refers to the privileges or immunities of the Houses of Parliament and the powers of the Houses of Parliament to protect the integrity of their processes.<sup>120</sup> Section 49 of the *Australian Constitution* gives the Australian Parliament power to declare the 'powers, privileges and immunities' of the Houses of Parliament and provides that, in the absence of any declaration by the Parliament, the powers, privileges and immunities held by the United Kingdom's House of Commons at the time of the establishment of the Commonwealth shall apply.

2.101 There are two aspects of parliamentary privilege. The first is set out in art 9 of the *Bill of Rights 1688* (UK) (which is applied in Australia by virtue of s 49 of the Constitution), which states: 'That the freedom of speech and debates or proceedings in Parliament ought not to be impeached or questioned in any court or place outside Parliament'. Article 9 confers an immunity from civil or criminal action and examination in legal proceedings on members of the Houses, witnesses and others taking part in proceedings in parliament. The *Parliamentary Privileges Act 1987* (Cth) clarifies that giving evidence or submitting a document to a House or committee are 'proceedings in parliament' covered by the immunity. The second aspect of parliamentary privilege is the parliament's power to conduct inquiries, including the ability to compel witnesses to give evidence or produce documents.

2.102 It is generally accepted that a general secrecy provision will not prevent the disclosure of information to the Parliament or a parliamentary committee.<sup>121</sup> A practical illustration was recently given in the Explanatory Memorandum released by

<sup>117</sup> Clerk of the Senate, *Submission SR 03*, 23 January 2009. See H Evans (ed), *Odgers' Australian Senate Practice* (12th ed, 2008), 51–55 for a discussion of the application of secrecy provisions to parliamentary inquiries.

<sup>118</sup> Clerk of the Senate, *Submission SR 03*, 23 January 2009.

<sup>119</sup> Ibid.

<sup>120</sup> H Evans (ed), *Odgers' Australian Senate Practice* (12th ed, 2008), Ch 2.

<sup>121</sup> Ibid, 51.

Treasury with the Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill, Exposure Draft, in March 2009 (Tax Laws Exposure Draft Bill):

While parliamentary privilege is commonly considered to protect disclosures of information made during parliamentary proceedings, such privilege also protects disclosures of information for the purpose of such proceedings. For instance, under parliamentary privilege the ATO can currently provide taxpayer information to ministers for the purpose of briefing the minister to respond to questions in Parliament (in the form of questions on notice and in question time briefs) and can also provide information to parliamentary committees when requested.<sup>122</sup>

2.103 The effect of parliamentary privilege in this context, however, is that where information is provided and presented in Parliament, while the person presenting the information may be covered by the immunity that privilege provides, personal information—and other information—may effectively become public. As this may not always be the desired consequence, Parliament may choose to abrogate parliamentary privilege and prevent the disclosure of information to the Parliament or its committees.<sup>123</sup>

2.104 An example of expressly dealing with parliamentary privilege is seen in the Tax Laws Exposure Draft Bill. As noted in the Explanatory Memorandum:

As the exposure draft seeks to provide for the only circumstances in which taxpayer information can be disclosed to ministers and the Parliament, ... the operation of parliamentary privilege is specifically excluded.<sup>124</sup>

2.105 The following illustration is provided:

The Treasurer is asked a question about the tax affairs of a particular taxpayer and seeks to obtain this information for the purpose of responding to that question during the sitting of Parliament. In these circumstances, the ATO cannot provide any taxpayer information to the Treasurer for this purpose, because such disclosures are not permitted by the exposure draft.<sup>125</sup>

---

122 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.24].

123 An intention to abrogate parliamentary privilege requires express statutory words: H Evans (ed), *Odgers' Australian Senate Practice* (12th ed, 2008), 53; G Griffith, *Parliamentary Privilege: Major Developments and Current Issues*, NSW Parliamentary Library Research Service Background Paper No 1/07 (2007), 82–84.

124 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.25]. The relevant provisions are Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), cl 355-60.

125 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), 36–37, Example 4.28.

2.106 However, where the issue is the power to compel the giving of evidence, the position is different:

Since the purpose of the [proposed] framework is to specify the circumstances in which a taxation officer and non-taxation officer *may* disclose information to a minister or the Parliament and to recognise other powers and laws that can be used to compel the production of information, the framework accordingly does not override Parliament's power to *compel* the production of information.<sup>126</sup>

2.107 There are some secrecy provisions that prevent the Parliament compelling the production of certain information. For example, s 37(3) of the *Auditor-General Act 1997* (Cth) provides that the Auditor-General cannot be required, and is not permitted, to disclose information that he or she is prohibited from including in a public report to a House of Parliament, a member of a House of the Parliament, or a parliamentary committee. The Explanatory Memorandum to the Act makes clear that 'the effect of [this subclause] is to act as a declaration for the purposes of section 49 of the Constitution'.<sup>127</sup>

2.108 Section 503A of the *Migration Act 1958* (Cth) provides a further example. Subsections 503A(2)(c) and (d) prohibit ministers or officers who have received certain confidential information from a law enforcement or intelligence agency from being required to disclose the information to a parliament or parliamentary committee. Provisions of the *Migration Act 1958* (Cth) and the *Inspector of Transport Security Act 2006* (Cth) also regulate the permissible content of reports to parliament.<sup>128</sup>

2.109 In its drafting direction dealing with secrecy provisions, the Office of Parliamentary Counsel (OPC) advises that secrecy provisions that extend to information that may be the subject of inquiry by the Parliament or a parliamentary committee should specify the circumstances in which that information may be disclosed. The OPC suggests that this could be done, in appropriate cases

by including a definition at the end of the secrecy provision to make clear that 'the performance of duties under the Act' includes the giving of evidence to Parliament or to a parliamentary committee.<sup>129</sup>

#### *ALRC's views*

2.110 In this Inquiry, the ALRC is asked to consider laws and practices relating to the protection of Commonwealth information, including consistent and workable laws in relation to secrecy. The interaction between secrecy provisions and parliamentary privilege is one aspect of the workability of secrecy provisions.

---

126 Ibid, [4.26]; and see Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) cl 350-60(3), 355-195(3).

127 Auditor-General Bill 1996 Explanatory Memorandum, [71].

128 See, eg, *Inspector of Transport Security Act 2006* (Cth) ss 64(2), 64(3), 64(4), 64(5); *Migration Act 1958* (Cth) ss 46A(5), 46B(4), 46B(5), 72(5), 91F(4), 91L(4), 91Q.

129 Parliamentary Counsel, *Drafting Direction No 3.5: Offences, Penalties, Self-Incrimination, Secrecy Provisions and Enforcement Powers*, Office of Parliamentary Counsel, 13 November 2007, [61].

2.111 The ALRC notes that, when drafting secrecy provisions, the Australian Government should give attention to the interaction between the provision and other laws and practices, including parliamentary privilege. Where it is intended to abrogate parliamentary privilege so as to prevent the disclosure of information to the Parliament, this intention should be clearly stated in the provision and supporting documents, as for example in the Tax Laws Exposure Draft Bill.<sup>130</sup>

2.112 The ALRC considers that the current OPC Drafting Direction No 3.5 adequately draws attention to the need to clarify the application of a secrecy provision to the disclosure of information to the Parliament or a parliamentary inquiry. In Chapter 13 the ALRC considers a range of matters to be included in a drafting direction concerning secrecy provisions. This direction would be a suitable place also to include drafting guidance in relation to parliamentary privilege.

## The public interest

### Background

2.113 The challenge for the ALRC in this Inquiry is to strike the right balance between the public interest in open and accountable government and particular identified public interests—such as privacy, commercial confidentiality, national security, law enforcement and investigation. In doing so, the ARTK coalition urged the ALRC

to return to first principles in its report by recommending a system that is practical and effective in ensuring information is open to all Australian citizens. The enshrinement of the right to access and sharing of information has the additional benefit of raising awareness and educating the public as to the operation of its government. There is a good deal of evidence from overseas that open access to information strengthens the democracy, confidence in government policy formulation and action.<sup>131</sup>

2.114 Such ‘first principles’ require a focus on the idea of the public interest, both in the general sense of an overriding justification for government action as a balance of openness and the protection of relevant information—including through secrecy provisions; and the specific sense of those matters that are regarded as so essential, or reflective of ‘essential public interests’, as to require specific protection through secrecy provisions.

2.115 The emphasis on public interest has recently been brought to the forefront by Senator Faulkner in announcing the FOI Exposure Draft Bill, that ‘[q]uestions of openness, and confidentiality, have to be treated as different aspects of the same overriding obligation to act *in the public interest*’.<sup>132</sup>

<sup>130</sup> Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth).

<sup>131</sup> Australia’s Right to Know, *Submission SR 35*, 6 March 2009.

<sup>132</sup> J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

2.116 What amounts to public interest has also been the subject of consideration by the House of Representatives Standing Committee on Legal and Constitutional Affairs (House of Representatives Standing Committee), chaired by Mark Dreyfus QC MP, which recommended in its *Whistleblower Protection* report that the Australian Government introduce legislation, entitled the Public Interest Disclosure Bill, to provide whistleblower protections in the Australian Government public sector.<sup>133</sup>

2.117 In this Inquiry, the ALRC seeks to articulate how best to identify the relevant public interests that justify protection through the mechanism of secrecy provisions and/or other mechanisms concerning information handling. As ‘public interest’, both in the general and narrower senses, is a recurring theme, the following section provides a consideration of how public interest may be seen in legislation and different approaches that may be taken in relation to it.

### **A wide concept**

2.118 Where a specific ‘public interest’ test has arisen for consideration as a statutory concept in proceedings, a wide approach has been taken. For example, in *Australian Broadcasting Tribunal v Bond*, in reviewing a decision by the Australian Broadcasting Tribunal, the High Court held that in construing references to public interest in a statute the court should adopt a wide definition and the considerations to be taken into account were not to be ‘closely confined’.<sup>134</sup> Similarly, in *Right to Life Association (NSW) Inc v Secretary, Department of Human Services and Health*, Lockhart J noted that the ‘public interest is a concept of wide meaning and not readily delimited by precise boundaries’.<sup>135</sup>

2.119 As noted in the review of the FOI Act by the ALRC and the Administrative Review Council (ARC) in 1995, *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), the public interest is ‘an amorphous concept’, undefined in the FOI Act or any other Act.<sup>136</sup> Saying that something ‘is in the public interest’ is also a different concept from something that is ‘of interest to the public’.<sup>137</sup>

---

133 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 1.

134 *Australian Broadcasting Tribunal v Bond* (1990) 170 CLR 321, 381–2.

135 *Right to Life Association (NSW) Inc v Secretary, Department of Human Services and Health* (1995) 128 ALR 238, 245, a case concerning legislation regulating the administration of clinical trials that made reference to ‘public interest’ considerations to justify a decision to oppose a particular procedure in the instant case.

136 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [8.13].

137 *Johansen v City Mutual Life Assurance Society Ltd* (1905) 2 CLR 186.

2.120 The width of the idea of public interest was acknowledged in the *Whistleblower Protection* report:

Like the term whistleblower, the term ‘public interest’ can be defined in a number of ways and in a number of contexts. Indeed, it may not be possible to arrive at an all encompassing definition of the public interest.<sup>138</sup>

2.121 Wide concepts, however, are not precise ones and this may provide room to argue ‘public interest’ from both directions—namely, that information should be withheld, or protected by secrecy, in the public interest; and that information should be revealed in the public interest.<sup>139</sup> While there are similar areas of public interest concern in the FOI Act and the proposed Public Interest Disclosure Bill, in the FOI Act public interest arguments are seen in support of resisting disclosure, while in the whistleblowing context public interest is used in support of revelation of information.

### A unifying thread

2.122 The ‘public interest’ may be found as a backdrop for, or specific element in, legislation. For example, in relation to the FOI Act, it has been commented that ‘notions of public interest constitute the basic rationale for the enactment of, as well as the unifying thread running through the provisions of, the FOI Act’.<sup>140</sup>

2.123 So, for example, it may be said that the FOI Act reflects the broad public interest in open and accountable government. But ‘public interest’ is also included in a number of ways in several of the exemption provisions in the Act. It is implicit that the protection of Commonwealth information is necessary in certain circumstances, such as national security—as reiterated by Senator Faulkner in announcing the FOI Exposure Draft Bill.<sup>141</sup> The role of public interest in the context of the exemption provisions is also brought more into prominence in the Draft Bill through a reformulation of the public interest test. As explained in the *Companion Guide* released with the Exposure Draft Bill, it is a single test, ‘weighted in favour of disclosure of documents’, which will require access to the requested documents ‘unless (in the circumstances) access to the document at that time would, on balance, be contrary to

138 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), [2.34].

139 Ibid [2.34]–[2.44] provides a discussion of submissions received by the Standing Committee on this issue.

140 Eccleston and Department of Family Services and Aboriginal and Islander Affairs (1993) 1 QAR 60, 74.

141 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

the public interest'.<sup>142</sup> The Bill also includes factors that must not be taken into account and those which favour disclosure.<sup>143</sup> The FOI Act is considered further in Chapter 4.

2.124 In the context of secrecy provisions, ideas of public interest are found both implicitly and expressly. The public interest is an explicit element of some secrecy provisions—for example, it is only an offence under s 58 of the *Defence Force Discipline Act 1982* (Cth) where the unauthorised disclosure of information is likely to harm ‘the security or defence of Australia’. In such examples, while the term ‘public interest’ is not used, the matter protected expressly reflects public interest in a particular, identified area.

2.125 The public interest may also be raised as a ground for claiming immunity for the production of documents in court proceedings. Such a claim to ‘public interest immunity’ may be made both under the common law<sup>144</sup> and under s 130 of the *Evidence Act 1995* (Cth).<sup>145</sup>

2.126 Similar claims to public interest immunity are able to be made before a parliamentary inquiry, such as a committee, where the executive government or a minister can object to disclosure of information on the basis of ‘executive’ or ‘public interest’ immunity. The grounds of public interest immunity that may be claimed before a parliamentary inquiry are those contained within the FOI Act.<sup>146</sup>

2.127 The proposed Public Interest Disclosure Bill also seeks to include public interest as a defence to the disclosure of information, recognising that ‘it is in the public interest that accountability and integrity in public administration are promoted by identifying and addressing wrongdoing in the public sector’.<sup>147</sup> The House of Representatives Standing Committee recommended that the types of disclosures to be protected in this public interest should

include, but not be limited to serious matters related to:

- illegal activity;
- corruption;
- maladministration;
- breach of public trust;

---

<sup>142</sup> J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009), 11.

<sup>143</sup> Ibid.

<sup>144</sup> See eg *Sankey v Whitlam* (1978) 142 CLR 1, 38 (Gibbs ACJ).

<sup>145</sup> Section 130 is replicated in the other uniform Evidence Acts: *Evidence Act 1995* (NSW), *Evidence Act 2008* (Vic), *Evidence Act 2001* (Tas), *Evidence Act 2004* (NI).

<sup>146</sup> Parliament of Australia—Senate, *Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters* (1989).

<sup>147</sup> Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), xix.

- 
- scientific misconduct;
  - wastage of public funds;
  - dangers to public health;
  - dangers to public safety;
  - dangers to the environment;
  - official misconduct (including breaches of applicable codes of conduct); and
  - adverse action against a person who makes a public interest disclosure under the legislation.<sup>148</sup>

2.128 While stating that ‘new legislation on public interest disclosures should have a clear and simple purpose so that anyone who reads the Act can immediately discern its intent’,<sup>149</sup> the House of Representatives Standing Committee concluded that:

The term public interest need not be explicitly defined, but rather reflected in the purpose of the legislation and its provisions on disclosable conduct. ... The purpose and key principles of the legislation ... should be included in a preamble to the Bill.<sup>150</sup>

2.129 Rather than being stated with any precision, public interest disclosures are left described in somewhat opaque terms as ‘serious matters’ relating to the non-exclusive list of subjects noted above.

### Contrasting approaches

2.130 In reviewing secrecy laws and considering proposals for reform, two contrasting approaches are, on the one hand, to consider the category of information justifying secrecy—or at least secrecy obligations warranting criminal sanctions; and, on the other, to consider the public interests that justify secrecy in particular cases.

2.131 As noted in Chapter 1, the Gibbs Committee recommended that the general offence provisions in the *Crimes Act* should be repealed, and that:

the application of criminal sanctions under the general criminal law of the Commonwealth to disclosure of official information should be limited to certain categories of information and that these should be no more widely stated than is strictly required for the effective functioning of Government.<sup>151</sup>

2.132 The Gibbs Committee went on to consider what categories of information should be protected by criminal sanctions. These included information relating to intelligence and security services; defence; foreign relations; information obtained in confidence from other governments or international organisations; and information the

---

148 Ibid, xxi, Rec 7.

149 Ibid, [2.45].

150 Ibid, [2.49].

151 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 317.

disclosure of which affects law enforcement.<sup>152</sup> Where information related to defence or foreign relations, or was obtained in confidence from foreign governments and international organisations, it was necessary to prove that the disclosure caused damage; but in relation to other categories, such proof was not necessary.<sup>153</sup> Further, the list of protected categories of information was not to include certain matters, unless otherwise covered under the other heads:

- (i) information obtained by one or other form of interception of communications or information as to the processes of interception;
- (ii) information supplied in confidence;
- (iii) information the disclosure of which could damage Commonwealth/State relations;
- (iv) Cabinet documents;
- (v) information affecting personal privacy; or
- (vi) information causing damage to the economy.<sup>154</sup>

2.133 Alternatively, one can view the identification of particular categories of information as reflecting an underlying recognition of particular—or essential—public interests served by maintaining secrecy provisions in certain areas. An example of an attempt at definition is that found in s 24 of the *Surveillance Devices Act 1998* (WA), which defines ‘public interest’ as including:

the interests of national security, public safety, the economic well-being of Australia, the protection of public health and morals and the protection of the rights and freedoms of citizens.

2.134 In the AGD’s response to the questions in IP 34 about whether secrecy laws were still relevant and necessary in the light of freedom of information laws and other modern moves towards greater openness and accountability on the one hand, and the current international security environment on the other,<sup>155</sup> considered above, the AGD made additional comments with respect to the approach to protecting information.

2.135 While endorsing the importance of openness, the AGD submitted that ‘[i]t is necessary for certain information to be protected by strong laws, involving criminal penalties, to ensure the public interest is not harmed by its disclosure’.<sup>156</sup> The AGD then suggested the kinds of information that should be protected as government information from general disclosure:

<sup>152</sup> Ibid, 317–321.

<sup>153</sup> Ibid, 31.50 (a)–(d). In the case of information relating to the intelligence and security services disclosed by someone who was not a member or ex-member of those services, proof of damage was necessary: 31.50 (d)(ii).

<sup>154</sup> Ibid, 332, 31.50 (e).

<sup>155</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 1–1.

<sup>156</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

- information that could prejudice Australia's national security, defence or international relations
- information that could endanger life
- information that could prejudice law enforcement operations and the effective working of law enforcement agencies
- information provided to the government in confidence by foreign government agencies
- Cabinet documents, and
- other information that could prejudice the effective working of Government.<sup>157</sup>

### ALRC's views

2.136 As evident in the discussion in this chapter, FOI and secrecy are interrelated facets of the government information prism. The Solomon Committee stated that '[t]he public interest is the central, unifying feature of freedom of information'.<sup>158</sup> In this regard it may be commented that the public interest is also the central, unifying feature of secrecy laws. As noted above, Senator Faulkner expressed this in terms of obligation, that openness and confidentiality should be seen as 'different aspects of the same overriding obligation to act *in the public interest*'.<sup>159</sup>

2.137 In its review of the FOI Act in 1995, the ALRC and ARC commented that '[t]he availability of government information should be determined by the public interest'.<sup>160</sup> In the context of this Inquiry it may similarly be said that the protection of government information through secrecy laws should be determined by the public interest.

2.138 Any review of secrecy laws must, therefore, test existing provisions against a backdrop of public interest. Where particular provisions do not match, or cannot be justified in accordance with identifiable public interests, then they must be judged wanting and recommendations made for their recasting or repeal. A particular challenge in this Inquiry is to consider when, and what kinds of, public interest elements should be expressly included in secrecy provisions.

2.139 In this Discussion Paper the ALRC proposes a reworking of the conceptual approach reflected in secrecy provisions through the public interest lens of harm, rather than simply by reference to categories of information. As noted above, the Gibbs

---

157 Ibid.

158 Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), 1.

159 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

160 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), 95.

Committee recommendations took this latter approach, with proof of harm being required in certain cases.

2.140 While it may be argued that starting from a category of information ‘relating to defence’ and requiring the prosecution to prove damage—as suggested by the Gibbs Committee—is similar to requiring proof that the disclosure is likely to harm Australia’s defence, they reflect a different approach to public interest and, therefore, a different underlying rationale.

2.141 The areas in which an overriding notion of public interest requires a protection of information is largely in agreement, both in the submissions and in prior reviews, and is consistent, for example, with the approach in the AGD list which focuses, in the main, on information, the disclosure of which may cause harm in particular ways.

2.142 The weakness of a ‘categories of information’ approach, however, is that it is indiscriminate. While each category may be seen as reflecting a sense of public interest—namely, that disclosure of information of that kind is inherently, or potentially, harmful—the emphasis is not on the harm, but on the category. And, in such a case, a desire for secrecy can drive the classification of information in particular ways—a problem identified in the FOI context where an alleged overuse of the class exemption for Cabinet documents, for example, has attracted criticism.<sup>161</sup>

2.143 As the nature, place and meaning of public interest has been considered actively in the context of the FOI Act, an analysis of the Act and public interest provides an instructive prelude to a consideration of the role of public interest, and balancing public interests, in secrecy laws. The public interests indentified in the FOI Act are considered as a component of both the general secrecy offence in Chapter 6, and the administrative secrecy provision set out in Chapter 13.

---

161 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.58]–[8.61]; Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), ch 8, describing the Cabinet exemption in Queensland as ‘a bolt hole’.<sup>107</sup> See also Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), ch 4.

### **3. Sharing Commonwealth Information**

---

#### **Contents**

Introduction	79
Framework for information sharing	81
Security classification system	81
Memorandums of understanding	84
Agency information-handling policies	86
Trusted Information Sharing Network	87
Conflicting obligations	88
Outcomes of information sharing	90
Data matching	90
Other outcomes of information sharing	94
Submissions	95
ALRC's views	103

#### **Introduction**

3.1 The Terms of Reference for this Inquiry require the Australian Law Reform Commission (ALRC) not only to have regard to the importance of balancing the need to protect Commonwealth information and the public interest in an open and accountable system of government, but also to have regard to the increased need to share such information within and between governments and with the private sector.<sup>1</sup>

3.2 The previous chapter discussed the concept of ‘open government’ and the need for the Australian Government to share information with, or make information available to, the public at large, or particular members of the public, in order ‘for the people to know whether a government’s deeds match its words’.<sup>2</sup>

3.3 This chapter focuses on information sharing for the purpose of satisfying governmental policies and programs. Normally, this will involve the communication of information between Australian Government agencies. However, given privatisation, public-private partnerships and concerns about critical infrastructure, Australian

---

<sup>1</sup> See Terms of Reference at the front of this Discussion Paper.

<sup>2</sup> J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

Government agencies increasingly need to share information outside of government, with state and territory agencies or the private sector.

3.4 Information, as Greg Terrill has commented, ‘underpins almost all of government activity’; it is both an ‘object in its own right’ and ‘a dimension of all government activity’.<sup>3</sup> Information can be shared through a range of mechanisms, including, for example, data matching; legislative codification of permissible sharing; and memorandums of understanding (MOUs). Overlying such mechanisms may be seen to be a broad concept of what is described as a ‘whole of government’ approach, which refers to ‘coordinated activities of government that cross jurisdictions’.<sup>4</sup>

3.5 In its 2004 report, *Connecting Government: Whole of Government Responses to Australia’s Priority Challenges*, the Australian Government’s Management Advisory Committee defined ‘whole of government’ in the Australian Public Service (APS) as denoting:

public service agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues. Approaches can be formal and informal. They can focus on policy development, program management and service delivery.<sup>5</sup>

3.6 In his preface to the report, Dr Peter Shergold described ‘whole of government’ as

the public administration of the future. It offers links and connections to the global community of ideas, knowledge and understanding essential for the APS to face the governance challenges of the 21<sup>st</sup> century. It extols team-based approaches to solving the wicked problems that are endemic to public policy.<sup>6</sup>

3.7 The idea of a whole of government approach requires that secrecy provisions be considered within a much wider framework of information policy. In its response to the report of the Independent Review Panel examining the Queensland *Freedom of Information Act 1992*, the Queensland Government committed to developing

a whole-of-government information policy framework that will set the long term goals and strategic direction for government information policy, while at the same time mapping the immediate priorities for government in seeking to position itself as an innovative and accountable custodian of government information.<sup>7</sup>

---

3 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 3, 5.

4 Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia’s Priority Challenges* (2004), 2. The Management Advisory Committee is a forum of Secretaries and Agency Heads established under the *Public Service Act 1999* (Cth) to advise the Australian Government on matters relating to the management of the Australian Public Service (APS): see <http://www.apsc.gov.au/mac/index.html>.

5 Ibid, 4.

6 Ibid, vi.

7 Queensland Government, *The Right to Information: A Response to the Review of Queensland’s Freedom of Information Act* (2008), 3.

3.8 Such a response conceptualises freedom of information, secrecy provisions and information management as different facets of a much larger information prism in which the government has particular responsibilities as a ‘custodian’ of information in a context of accountability.

## Framework for information sharing

3.9 Information sharing sits within the overall framework of information management. Any sharing of Commonwealth information must either be authorised or excepted from the ambit of any applicable secrecy provisions. This section of the chapter considers aspects of the framework for information sharing, including: the system for the classification of documents on the basis of their security sensitivity; memorandums of understanding; agency information-handling policies; and the ‘Trusted Information Sharing Network’ for sharing information with the private sector.

### Security classification system

3.10 The classification of information according to different levels of security under the *Australian Government Protective Security Manual* (PSM)<sup>8</sup> is a key way in which the flow of information is regulated in the public sector. The PSM sets out guidelines and minimum standards in relation to protective security for Australian Government agencies and officers, and for contractors who perform services for or on behalf of the Australian Government.<sup>9</sup> It is periodically revised by the interdepartmental Protective Security Policy Committee.

3.11 Part C of the PSM deals with information security. That part provides agencies with guidance on the development of security policies that address awareness, responsibility, behaviour and deterrence to ensure official information is not compromised. The ALRC considered Part C of the PSM in detail in its 2004 report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98). In that report, the ALRC noted that Part C sets out the following information security principles:

- the availability of information should be limited to those who need to use or access the information to do their work (the ‘need to know’ principle);
- where the compromise of information could cause harm to the nation, the public interest, the government or other entities or individuals, agencies must consider giving the information a security classification;

---

<sup>8</sup> Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM) [Summary]* (2006) <<http://www.ag.gov.au>> at 15 October 2008.

<sup>9</sup> Ibid.

- once information has been identified as requiring security classification, a protective marking must be assigned to the information;
- once information has been security classified, agencies must observe the minimum procedural requirements for its use, storage, transmission and disposal.<sup>10</sup>

3.12 The PSM distinguishes between national security information and non-national security information. ‘National security information’ includes any official resource that records information about, or is associated with, Australia’s security, defence, international relations, or national interest. National security information may be given one of four security markings:

- **Restricted**—if compromise of it could cause ‘limited damage’ to national security;
- **Confidential**—if compromise of it could cause ‘damage’ to national security;
- **Secret**—if compromise of it could cause ‘serious damage’ to national security;
- **Top Secret**—if compromise of it could cause ‘exceptionally grave damage’ to national security.<sup>11</sup>

3.13 ‘Non-national security information’ includes any official resource that threatens the interests of important groups or individuals other than the nation. Non-national security information may be given one of three security markings:

- **X-in-Confidence**—if compromise of it could cause ‘limited damage’ to the Commonwealth, the Government, commercial entities or members of the public;
- **Protected**—if compromise of it could cause ‘damage’ to the Commonwealth, the Government, commercial entities or members of the public;
- **Highly Protected**—if compromise of it could cause ‘serious damage’ to the Commonwealth, the Government, commercial entities or members of the public.<sup>12</sup>

3.14 Security classified information may only be accessed and handled by persons who have obtained a sufficient security clearance. The clearance process aims to identify whether there is anything in an individual’s behaviour or history that indicates

---

<sup>10</sup> Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004) Ch 4. ‘Minimal procedural requirements’ include, eg, taking precautions to ensure that only people with a demonstrated need to know and the appropriate security clearance gain access to security classified information; and providing a document registration system to identify all security classified information held by the agency.

<sup>11</sup> Ibid, [2.9].

<sup>12</sup> Ibid, [2.12].

that he or she would be a security risk. Security clearances for non-national security information—Clearances for a Position of Trust—are conducted by individual Australian Government agencies. However, Designated Security Assessment Positions—which allow access to national security information—require an assessment from the Australian Security Intelligence Organisation (ASIO).<sup>13</sup>

3.15 The Australian Government's stated policy is to keep security classified information to the necessary minimum.<sup>14</sup> However, in a 1999 report on the operation of the classification system for protecting sensitive information, the Australian National Audit Office noted that all audited agencies incorrectly classified files, with over-classification being the most common occurrence.<sup>15</sup> Ongoing problems with the classification system were also raised in a number of submissions in response to the Issues Paper, *Review of Secrecy Laws* (IP 34).<sup>16</sup>

3.16 A post on the ALRC's online forum, *Talking Secrecy*, conducted during the Inquiry, identified difficulties caused by the 'Restricted' classification level. It advised that, because most of Australia's allies do not have an equivalent level of protection (moving straight from 'Unclassified' to 'Confidential'), information that may be classified as 'Restricted' in Australia may be upgraded to 'Confidential' in the United States and then up to 'Secret' on return to Australia. The post also advised of confusion surrounding the 'Unclassified' category. Some people understand this to mean information that has not yet been assessed for classification, whereas the correct meaning is information that has been assessed as not requiring a security classification.<sup>17</sup>

3.17 In ALRC 98, the ALRC made a number of recommendations with regard to the PSM and the classification of Commonwealth information, including that:

- the PSM should be amended to provide further and more explicit guidance on the different classification levels, how to make classification decisions and when such decisions require review by a more senior officer,<sup>18</sup>

---

13 Ibid, Ch 6 discusses security clearances.

14 Ibid, [2.10].

15 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Audit Report 7 (1999), [2.84].

16 Whistleblowers Australia, *Submission SR 40*, 10 March 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009; Australian Press Council, *Submission SR 16*, 18 February 2009.

17 'Talking Secrecy' Post.

18 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 4–3.

- Australian Government agencies should ensure that all staff required to make classification decisions are well trained in classification policy and procedure;<sup>19</sup> and
- the mandatory minimum standards in the PSM should include express statements that information should only be classified when there is a clear and justifiable need to do so; the decision to classify should be based on the criteria set out in the PSM; and information should not be classified for extraneous reasons, such as to conceal breaches of the law or to prevent embarrassment to a person, organisation or agency.<sup>20</sup>

3.18 The ALRC further recommended that the PSM (with any sensitive protective security information removed) should be placed in the public domain<sup>21</sup>—as is the case in most comparable jurisdictions, such as the United States, Canada and New Zealand.<sup>22</sup> In its submission in response to IP 34, the Australian Press Council also called for the PSM to be declassified and made publicly available.<sup>23</sup>

3.19 The PSM has been revised since the publication of ALRC 98. Unfortunately, however, and without explanation, the document was subsequently given a security classification. The security classification scheme in the revised PSM is broadly consistent with the regime discussed above.<sup>24</sup>

3.20 In a submission to this Inquiry, Liberty Victoria proposed a simplified classification system for documents, with documents marked as either ‘National Security Information’ (NSI) or ‘non-NSI’. Liberty Victoria also supported the position taken in ALRC 98, that the PSM should

provide explicit classification guidance and information should only be classified (at any level) where there is a clear and justifiable reason for doing so. The later classification of the PSM is an ironic example of over classification; one which illustrates the absurdity of creating a system, which is inaccessible by either its intended or potential users.<sup>25</sup>

### **Memorandums of understanding**

3.21 An MOU does not, in itself, provide a legal basis for the handling of Commonwealth information—its terms must be underpinned by common law or statute. The Australian Government Attorney-General’s Department (AGD) described

19 Ibid, Rec 4–4.

20 Ibid, Rec 4–5.

21 Ibid, Rec 4–1. At the time of ALRC 98, the PSM did not have a security classification but was not publicly available.

22 Ibid, [4.17].

23 Australian Press Council, *Submission SR 16*, 18 February 2009.

24 Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM)* (2005).

25 Liberty Victoria, *Submission SR 19*, 18 February 2009.

them as ‘voluntary arrangements ... premised upon a willingness to enter into arrangements of mutual benefit and long term cooperation’.<sup>26</sup> While acknowledging that MOUs generally do not have the force of law, the Administrative Review Council has advised that they may regulate the exchange of information among government agencies by ‘formalis[ing] the terms of a relationship or framework for cooperation between the parties’.<sup>27</sup>

3.22 In its submission to this Inquiry, the Australian Transaction Reports and Analysis Centre (AUSTRAC) noted the importance of MOUs, backed up by secrecy provisions, in the context of the sharing of information among foreign intelligence units:

As these MOUs are not enforceable, the secrecy provisions of the [*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act)] provide reassurance and certainty to [foreign intelligence units] that information provided to AUSTRAC will not be disclosed except in specified circumstances, and vice versa.<sup>28</sup>

3.23 While the MOU facilitates the sharing of information, it is the legislative secrecy provisions themselves which are critical:

The secrecy provisions of Division 4 of Part 11 of the AML/CTF Act enable the [Australian Federal Police], the [Australian Crime Commission], [the Australian Security Intelligence Organisation] and [Australian Secret Intelligence Service] to communicate AUSTRAC information to a foreign government if satisfied that the foreign country will protect the confidentiality of the information, control its use and use it only for the purpose that it was provided.<sup>29</sup>

3.24 Several Australian Government agencies have MOUs that are relevant to information handling. For example, the Australian Securities and Investments Commission (ASIC) has entered into an MOU with the Australian Government Financial Reporting Council, under which the entities agree (subject to any restrictions imposed by law) to ‘share information that they believe would be of assistance to the other in understanding their respective responsibilities under the law’.<sup>30</sup> Each agency agrees to provide information requested by the other in a timely manner.<sup>31</sup> They further agree to use ‘reasonable endeavours’ to notify the other of the existence of relevant information, notwithstanding that the information has not been requested.<sup>32</sup>

---

26 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

27 Administrative Review Council, *The Coercive Information-Gathering Powers of Government Agencies*, Report No 48 (2008), 65.

28 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

29 Ibid.

30 Australian Government Financial Reporting Council, *Memorandum of Understanding Between the Australian Securities and Investments Commission and the Financial Reporting Council* (2004) <[www.frc.gov.au/auditor/mou/MOU\\_ASIC.asp](http://www.frc.gov.au/auditor/mou/MOU_ASIC.asp)> at 28 May 2009 cl 4.1.

31 Ibid, cl 4.2.

32 Ibid, cl 4.3.

Commonwealth and state and territory police also have entered into a detailed MOU for the sharing of law enforcement information.<sup>33</sup>

**3.25 The AGD remarked that MOUs and similar instruments**

may be used to set out a shared understanding and guidelines for the communication, handling and protection of particular information by the parties to the MOU. They can provide a consistent, reliable and easily managed means of ensuring protection of sensitive Commonwealth information.<sup>34</sup>

**3.26 The place and function of MOUs in facilitating and regulating information flows between agencies and with the private sector is considered in Chapter 15.**

**Agency information-handling policies**

**3.27** The policies and practices adopted by agencies also play a critical part in facilitating information sharing. As noted in Chapter 15, they can play a positive role in protecting Commonwealth information by clarifying and standardising information-handling processes.

**3.28** As part of the *APS Values and Code of Conduct in Practice*, issued by the Australian Public Service Commission, agencies are advised to establish ‘clear policies and guidelines so that employees are aware of the provisions that govern the management of information’.<sup>35</sup> Among such provisions are the security classifications of the PSM. Agency information-handling policies are considered in detail in Chapter 15.

**3.29 In a submission in response to IP 34, the AGD commented that:**

Agency policies on information handling may be directed towards several outcomes, including providing practical guidance on any applicable secrecy laws as well as maintaining the integrity of information held by the agency. ...

The Protective Security Manual (PSM) and the Australian Government ICT Information Security Manual (ISM) are key documents that provide guidance on the handling, usage, storage and destruction, of all Commonwealth information. They provide the guidance and encourage the application of the policy and procedures necessary to protect Commonwealth information, material and other assets but do not provide specific penalties themselves. These manuals set out minimum standards and agencies may implement higher standards if necessary to meet their specific needs.<sup>36</sup>

---

<sup>33</sup> New South Wales Police and others, *Memorandum of Understanding between New South Wales Police, Victoria Police, Queensland Police, Western Australia Police, South Australia Police, Northern Territory Police, Tasmania Police, ACT Policing, Australian Federal Police and the CrimTrac Agency*.

<sup>34</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

<sup>35</sup> Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <[www.apsc.gov.au](http://www.apsc.gov.au)> at 23 September 2008, ch 3.

<sup>36</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

## Trusted Information Sharing Network

3.30 One example of an initiative to provide a means for cooperative sharing of information is the establishment of the Trusted Information Sharing Network (TISN), following a recommendation by the Australian Government's Business–Government Task Force on Critical Infrastructure in March 2002.

Since the TISN was launched in 2003, governments around the world have realised that terrorism is just one threat to critical infrastructure. The TISN has been instrumental in promoting the ‘all hazards’ approach to critical infrastructure protection. This takes into account all possibilities, natural or manmade—from fire, criminal activity or cyclone to terrorism, flood or pandemic.<sup>37</sup>

3.31 The TISN is made up of nine different business sector groups and the network provides ‘a safe environment where industry and government can share vital information on critical infrastructure protection and organisational resilience’.<sup>38</sup> The Critical Infrastructure Advisory Council, which oversees the groups, also reports to the Attorney-General, in this way communicating at a high level with government on, amongst other areas of significance, Australia’s counter-terrorism arrangements.

3.32 ‘Critical infrastructure’ refers to:

those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would adversely impact on the social or economic well-being of the nation or affect Australia’s ability to ensure national security.<sup>39</sup>

3.33 Critical Infrastructure Protection is ‘not a new discipline’, but a ‘coordinated blending of existing specialisations’, including:

- law enforcement and crime prevention
- counter terrorism
- national security and defence
- emergency management, including the dissemination of information
- business continuity planning
- protective security (physical, personnel and procedural)
- e-Security
- natural disaster planning and preparedness
- risk management

---

37 Trusted Information Sharing Network, *Trusted Information Sharing Network for Critical Infrastructure Protection [Home Page]* <<http://www.tisn.gov.au>> at 16 April 2009.

38 Ibid.

39 Trusted Information Sharing Network, *Critical Infrastructure Protection National Strategy* (2004), 1.

- 
- professional networking
  - market regulation, planning and infrastructure development.<sup>40</sup>

3.34 As a considerable proportion of critical infrastructure is privately owned—as much as 90% in some parts of Australia—the approach of the TISN is to facilitate private industry and government working together to raise awareness of infrastructure security risks and to ‘ensure that information and techniques required to assess and mitigate risks is readily available and freely exchanged’.<sup>41</sup>

3.35 Given that the TISN operates on the basis of information sharing, and that there are legitimate concerns about revealing what may be confidential commercial information, the creation and maintenance of a trusting environment for cooperation is essential. In this regard, the combination of the TISN Deed of Confidentiality and guidelines for the handling of potentially commercially sensitive and security-related information operates to ensure that confidential information is properly managed and reasonably protected from unauthorised use or disclosure.<sup>42</sup>

3.36 As the TISN’s ‘Fact Sheet’ about the confidentiality deed explains,

The definition of confidential information is not to be read as having meaning under the Commonwealth Protective Security Manual (PSM). ‘Confidential Information’ under the PSM refers predominantly to national security information, rather than the type of commercially-sensitive information that is disclosed in TISN, and is subject to certain security requirements not required for TISN confidential information.<sup>43</sup>

3.37 The deed provides assurance amongst private sector participants in the network. Government representatives are not required to sign it as they have existing statutory and other legal obligations for the handling of information—including secrecy provisions. However, all government representatives who participate in the TISN are required to sign a Government Representative Confidentiality Acknowledgement, to expressly acknowledge these obligations.<sup>44</sup>

### **Conflicting obligations**

3.38 There is often a tension between the ‘need to share’ information and handling information on a ‘need to know’ basis. Sharing information may also conflict with other obligations—such as the need to protect privacy. This tension was identified in a report in 1995 by the House of Representatives Standing Committee on Legal and Constitutional Affairs on the protection of confidential personal information:

On the one hand, an unregulated transfer of information has implications both in terms of privacy and breach of confidence. However, on the other hand, limits on the

---

40 Ibid, 2.

41 Ibid.

42 Ibid, 5.

43 Trusted Information Sharing Network, *Fact Sheet: TISN Deed of Confidentiality* (2007), 2.

44 Ibid, 3.

access of Commonwealth agencies to information may impede the agencies, particularly in relation to law enforcement and revenue protection.<sup>45</sup>

3.39 Sharing information may also amount to a contravention of secrecy laws, which can affect communication at different points in the information flow. A secrecy provision may restrict the disclosure or communication of information in certain circumstances.<sup>46</sup> Any such restriction can have an immediate or potential impact on information sharing.

3.40 The potential danger of improperly managed sharing arrangements was highlighted in the multi-agency Project Wickenby taskforce established to target particular allegations of tax fraud. After questions were raised as to the processes for managing the sharing of information between the Australian Taxation Office (ATO), the Australian Crime Commission (ACC) and the Australian Federal Police (AFP), an inquiry was conducted by Dale Boucher, which was reported to have ‘raised serious concerns about mismanagement and inappropriate collusion’ between these agencies.<sup>47</sup> Boucher concluded that although there was not a ‘culture in which tax information may be inappropriately disclosed to law enforcement agencies’, ‘there may be a gap between current policy and practice’. He noted that:

it does highlight serious concerns about staff who have been seconded between the ATO, [ACC] and AFP, an increasingly common initiative to share the expertise and knowledge of the agencies as part of the Project Wickenby investigations.<sup>48</sup>

3.41 In a submission to this Inquiry, the Commonwealth Ombudsman remarked that although information obtained for the purposes of an investigation is ‘protected by secrecy provisions in the Ombudsman Act and other legislation’,

Agencies are sometimes reluctant to allow access to information except in accordance with their own internal security classification procedures. The Ombudsman’s office

45 Australian Parliament—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), 59.

46 For example, while not directly concerning secrecy laws, the sharing of information between agencies in formulating Australia’s response to the terrorist attacks in Bali in 2002, was said to be hampered by the operation of the *Privacy Act*. One of the key difficulties was that agencies did not have a shared understanding of how the Act operated, particularly in times of crises: Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia’s Priority Challenges* (2004), 195.

47 P Durbin, ‘ATO lashed over privacy breaches’, *Australian Financial Review*, 23 April 2009, 1.

48 Ibid, 61. The sharing of information in a context such as investigations of alleged tax fraud also gives rise to the issue of procedural fairness, where the information concerned is confidential information and the sharing may have an adverse impact on the individual concerned: *Johns v Australian Securities Commission* (1993) 178 CLR 408. The requirement of procedural fairness may, however, be abrogated: eg, *Royal Commissions Act 1902* (Cth) s 9(11) which was amended by the *Royal Commissions Amendment (Records) Act 2006* (Cth) to enable the transfer of information obtained by Royal Commissions to investigatory and law enforcement bodies without the requirement to provide procedural fairness to persons who could be adversely affected.

and agencies have always been able to agree upon a course of action that resolves this tension, but it can hamper speedy investigation. It is an issue that warrants broader consideration.<sup>49</sup>

3.42 How best to manage the tension between the appropriate protection of information and information sharing is one of the challenges in this Inquiry.

## **Outcomes of information sharing**

### **Data matching**

3.43 A key reason for, and product of, information sharing is ‘data matching’, described by the Federal Privacy Commissioner as ‘the large scale comparison of records or files … collected or held for different purposes, with a view to identifying matters of interest’.<sup>50</sup> Agencies and organisations may wish to conduct data matching for a number of purposes, including detecting errors and illegal behaviour, locating individuals, ascertaining whether a particular individual is eligible to receive a benefit, and facilitating debt collection.<sup>51</sup>

3.44 The sharing of information through data matching may need to take place:

- where there is a crisis or national emergency;
- to better examine information held by government, by analysing and integrating information held across a number of different portfolios;
- to integrate service delivery, for example, between the ATO and Centrelink, or between Centrelink and a private employment service provider; and
- to manage areas of joint activity by encouraging the sharing of information with the Australian Government, across jurisdictions and with the private sector.<sup>52</sup>

3.45 Law enforcement and counter-terrorism are obvious areas where a sharing of information and data matching may be crucial. The terrorist attack on the World Trade Center in New York on 11 September 2001 not only had an impact on the security environment, it also heightened the debate about the ‘need to share’ information between agencies. A number of agencies may have different pieces of information which, if connected, might assist counter-terrorism investigations. As the

---

49 Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009.

50 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998).

51 Ibid, 2. R Clarke, ‘Computer Matching by Government Agencies: The Failure of Cost/Benefit Analysis as a Control Mechanism’ (1995) 4 *Information Infrastructure and Policy* 29, 33.

52 Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia’s Priority Challenges* (2004), 60.

Administrative Appeals Tribunal commented in *Re Mickelberg and Australian Federal Police*, it is in the public interest

that law enforcement agencies have speedy, accurate and secure systems of communication, both within an agency and between agencies especially where agencies have different fields of responsibility.<sup>53</sup>

3.46 In a submission to this Inquiry, the Australian Commission for Law Enforcement Integrity (ACLEI) said that ‘[a]s in many other areas of government, collecting, analysing and sharing information is at the heart of law enforcement activity’.<sup>54</sup>

In recent decades, digital data storage and retrieval systems have become powerful intelligence aids in the investigation of serious crime. Technology and enhanced cooperation between jurisdictions have enabled unprecedented sharing of information about individuals, groups, property and other assets, and events.

Together, these advances and the legal framework have allowed law enforcement officers to perform their legitimate work more quickly and effectively than has previously been the case.<sup>55</sup>

3.47 However, agencies wishing to undertake data-matching activities may be prevented from carrying out these activities both through the application of privacy principles and by secrecy provisions that prohibit Commonwealth officers from using or disclosing relevant information.<sup>56</sup> Further, where sharing is permitted, it may be accompanied, as ACLEI commented, ‘by community concerns about the purposes to which information is put, and the security of that information’.<sup>57</sup>

### ***Privacy principles***

3.48 Under the *Privacy Act 1988* (Cth), agencies and organisations are subject to additional forms of regulation in respect of their data-matching activities through privacy principles in relation to information handling.<sup>58</sup> Further, agencies undertaking data-matching programs that include the matching of tax file numbers are subject to the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the *Data-matching Program (Assistance and Tax) Guidelines* issued under that Act.

3.49 The Federal Privacy Commissioner has issued guidelines that address general data-matching activities of agencies and a number of agencies have agreed to comply

53 *Re Mickelberg and Australian Federal Police* (1984) 6 ALN N176.

54 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

55 Ibid.

56 The existing confusion about the extent to which privacy principles prevent the release of information in appropriate cases is referred to in Ch 4.

57 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

58 *Privacy Act 1988* (Cth) s 14, IPP 10 and 11 and *Privacy Act 1988* (Cth) Sch 3, NPPs 2 and 10. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [10.86]–[10.111]; and pt D on the Privacy Principles.

with them.<sup>59</sup> 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. The Federal Privacy Commissioner also undertakes research and monitors developments in data processing and computer technology (including data matching and data linkage) to help minimise any adverse effects of such developments on privacy.<sup>60</sup>

3.50 In summary, the guidelines require agencies to give public notice of any proposed data-matching program; prepare and publish a ‘program protocol’ outlining the nature and scope of a data-matching program; provide individuals with an opportunity to comment on matched information if the agency proposes to take administrative action on the basis of it; and destroy personal information that does not lead to a match. Further, the guidelines generally prohibit agencies from creating new, separate databases from information about individuals whose records have been matched.<sup>61</sup>

3.51 There are obvious privacy risks associated with data matching. In the guidelines, the Federal Privacy Commissioner notes that data matching may involve the:

- use of personal information for purposes other than for the reasons it was collected, and these purposes may not be within the reasonable expectations of the individuals about whom the personal information relates;
- examination of personal information about individuals about whom there are no grounds for suspicion, sometimes without the knowledge of those individuals; and
- retention of matched information by agencies for potential future use.<sup>62</sup>

59 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998). In 2007–2008, the Federal Privacy Commissioner was provided with agency protocols for 13 data-matching programs: Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2007–30 June 2008* (2008) 64–71.

60 *Privacy Act 1988* (Cth) s 27(1)(c). In addition, the Federal 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. The Federal Privacy Commissioner may report to the minister responsible for administering the *Privacy Act* about the results of any research into developments in data-matching or proposals for data matching: *Privacy Act 1988* (Cth) ss 27(1)(c), 32(1).

61 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998), [33]–[41], [42]–[47], [63], [69]. In Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), the ALRC suggested that the Office of the Privacy Commissioner could exercise its research and monitoring function to review the data-matching guidelines. The ALRC also recommended that the Office of the Privacy Commissioner develop and publish guidance for organisations that conduct data-matching activities: Rec 10–4.

62 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998), 2. See also P Durbin, ‘ATO lashed over privacy breaches’, *Australian Financial Review*, 23 April 2009, 1.

3.52 The Federal Privacy Commissioner also notes that data-matching is not always reliable. Matched information may fail to distinguish between individuals with similar details; input data may not be accurate; technical errors may occur; and fields may not be standardised.<sup>63</sup>

#### ***Secrecy provisions***

3.53 One significant issue is whether secrecy provisions inappropriately restrict data matching or other information sharing between agencies. For example, federal, state and territory governments are increasingly focusing on issues related to identity security.<sup>64</sup> Data matching may assist an agency to establish or verify an individual's identity to facilitate that individual's enrolment in an electronic system. Secrecy provisions could prevent data matching conducted for the purpose of detecting errors and identity fraud in existing systems.

3.54 In the 1995 review conducted by the House of Representatives Standing Committee on Legal and Constitutional Affairs, the Committee heard that secrecy provisions frequently impeded the flow of information from one department to another. In its evidence to the Committee, the AGD took the view that secrecy provisions were developed to prevent disclosure of official information to the public, but were too inflexible to meet the increasing need to transfer information within government, for example across the taxation, health and social security areas.<sup>65</sup>

3.55 More recently, the Treasury reviewed the secrecy provisions in taxation legislation (the Taxation Secrecy Review) and considered the need to balance taxpayer privacy against the need to facilitate government operations through information sharing. In that review it was noted that law enforcement agencies consider that current secrecy and disclosure provisions hinder the investigation and prosecution of serious crime, because taxpayer information provided by the ATO cannot be used as evidence in the prosecution of a non-tax related offence.<sup>66</sup>

3.56 Another issue raised in the Taxation Secrecy Review was whether the Commissioner of Taxation could obtain access to employee records of ATO

---

63 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998), 2.

64 Since April 2005, the AGD has been developing and implementing a National Identity Security Strategy, which comprises the national Document Verification Service and the e-Authentication framework: Council of Australian Governments (COAG), *Intergovernmental Agreement to a National Identity Security Strategy*, 13 April 2007; Australian Government Department of Finance and Deregulation, *Australian Government e-Authentication Framework for Individuals* (2008) <<http://www.finance.gov.au/e-government/security-and-authentication/agaf-i.html>> at 4 November 2008.

65 Australian Parliament—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), 61.

66 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 29.

employees. At present, the Commissioner of Taxation, when acting in his or her capacity as an agency head, can only gain access to employee tax information that has been obtained from a public source. It was suggested that amendments could be made to allow the Commissioner, in the capacity as an employer, access to taxation information about ATO officers or contractors. This would allow the Commissioner to be confident that all employees have complied with their tax obligations and thus ensure community confidence in the ATO.<sup>67</sup>

3.57 Following the Taxation Secrecy Review, the Government released the Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Tax Laws Exposure Draft Bill). A key aspect of the Bill is the inclusion of exceptions to the applicable secrecy provisions to facilitate information sharing:

Exceptions to the obligation not to disclose taxpayer information are necessary because information obtained by the Australian Taxation Office (ATO) needs to be used by the ATO to fulfil its role and can often be vital to other arms of government in performing their functions effectively. ...

Some new disclosures of information will also be introduced in instances where privacy concerns are outweighed by the public benefit of those disclosures.<sup>68</sup>

3.58 The proposed amendments will stipulate exceptions to secrecy provisions. This approach is also seen, for example, in s 130 of the *Health Insurance Act 1973* (Cth), which provides that information may only be disclosed for the purposes of that Act, but the minister responsible for administering the Act may authorise disclosure if it is necessary in the public interest to disclose it, or if the disclosure is in accordance with a purpose, person or authority prescribed in regulations.

### **Other outcomes of information sharing**

3.59 Information sharing goes beyond agencies working across portfolio boundaries:

A sound whole of government approach requires understanding of how programs and policies come together to affect particular communities, social groups, sectors of the economy and/or regions. ... Most whole of government priorities require close cooperation with external groups, such as community organisations, businesses and other jurisdictions. Moreover, understanding the different perspectives of external groups is essential to the government's desire to see policies and programs make a constructive contribution 'on the ground', as well as in managing the risks associated with new initiatives.<sup>69</sup>

3.60 With the increasing privatisation of government services, public and private sector bodies may need to work together on programs and policies:

---

67 Ibid.

68 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [1.3], [1.12].

69 Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia's Priority Challenges* (2004), 89.

Service delivery is often undertaken, consciously or by default, on a collaborative basis. This is particularly so if it is undertaken by Centrelink but also if it is contracted out. A non-government agency would, for instance, be expected to link all programs it delivers on behalf of government. One of the challenges here is that these agencies are often trying to make sense of the connections between programs and policy. One of the solutions is to try and form feedback loops between service delivery and the policy process to unlock the lessons learnt in service delivery.<sup>70</sup>

3.61 One outcome of the collaboration across government and with private sector bodies is that by maximising the potential of technology, service provision may become ‘seamless’, through ‘common standards and shared investment in high-priority data collections and definitions’.<sup>71</sup> Another outcome is a greater sense of public ‘ownership’ of policy:

Involving external players in policy development or the design of services and programs has many benefits. Policies and services will more closely meet public needs if they are developed with the help of people affected by them. Policies will be better informed and based on evidence. Involvement is also likely to improve acceptance of policy measures and satisfaction with services.<sup>72</sup>

## Submissions

3.62 In IP 34, the ALRC asked about any concerns arising from the interaction between secrecy provisions and data-matching laws and practices.<sup>73</sup> The ALRC also asked whether federal secrecy provisions inhibit unduly the sharing of information within and between law enforcement agencies, governments and between governments and the private sector.<sup>74</sup>

3.63 Stakeholders provided a range of views, giving examples of where secrecy provisions inhibited the sharing of information, and those where it did not; suggesting ways that better sharing could be achieved; but also identifying certain dangers inherent in information sharing.

### *Secrecy provisions inhibiting information sharing*

3.64 A problem identified by the AGD was that because many secrecy offences apply to Commonwealth officers or to officers of the relevant agency, ‘there may be uncertainty as to whether information will remain protected if shared outside the agency’. The AGD submitted that:

If secrecy laws were to be drafted in a way that protects information based upon the nature of the information, and not the fact that it is held or obtained by a particular

---

70 Ibid, 10.

71 Ibid, 16.

72 Ibid, 97.

73 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 7–6.

74 Ibid, Question 1–2.

officer or agency, this may assist the sharing of information while ensuring sensitive information can continue to be given adequate protection.

In relation to information collected by government agencies for service delivery and regulatory functions, the capacity for agencies to exchange information tends to rely on finding specific exceptions to the various secrecy laws, which are based on particular programs or agencies. This approach can result in ‘informational silos’ that may not reflect the actual need to share information across agencies with common responsibilities. Few agency operations are neatly contained within these artificial boundaries.<sup>75</sup>

3.65 The AGD acknowledged the problems created by secrecy provisions where they operate as agency-specific provisions. Such provisions can create inconsistencies between agencies about how those agencies can share information, and whether they are able to share information at all. In its submission, the ATO gave an example of how taxation secrecy provisions hindered their ability to share information effectively:

Taxation secrecy provisions do inhibit the ATO’s ability to share information with law enforcement agencies, other government agencies, and the private sector.

This can create practical problems where the ATO is trying to assist other agencies with non-tax related investigations, or where a non-tax remedy may assist the ATO to deal with a tax mischief.

For example, the Australian Securities and Investment Commission (ASIC) may be pursuing civil action in relation to a taxpayer under the *Corporations Act 2001*. The ATO is not permitted to disclose taxpayer information to ASIC for the purposes of the civil action, even though the civil action may actually have the flow-on effect of protecting taxation revenue.<sup>76</sup>

3.66 Some stakeholders, however, emphasised the importance of secrecy provisions in restricting the sharing of information. The Australian Bureau of Statistics (ABS), for example, while identifying the importance of being able to gain access to certain information from other agencies, highlighted the importance of limiting or tightly controlling the access to information held by the ABS.

Accessing information from other agencies is fundamental to the ABS’s statistical capability, as it enables the ABS to compile statistics it may not be able to produce from conducting surveys alone. For example, the ABS counts the Australian population each five years and then updates this count each quarter using, for example, information on births and deaths from the State Registrars of Births, Deaths and Marriages, and overseas passenger cards from the Department of Immigration and Citizenship.

In addition, it may be more efficient to use administrative data from another agency than for the ABS to conduct surveys to collect similar information. Based on knowledge developed through the relationship it has with its providers, the ABS believes most members of the community would prefer government agencies to use information they’ve already provided, rather than being asked repeatedly by different agencies to provide the same information. ...

---

<sup>75</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

<sup>76</sup> Australian Taxation Office, *Submission SR 13*, 16 February 2009.

In this context, it is important for the ABS to have, for statistical purposes, access to selected information collected by government authorities.

Current secrecy provisions in the [*Census and Statistics Act 1905* (Cth) (CSA)] provide strong restrictions on the ABS sharing identifiable information it has obtained under the CSA. As discussed, this position is non-negotiable, as a guarantee of secrecy to data providers is fundamental to the quality of national statistics. Other agencies may also have secrecy provisions in their governing legislation, and this is an issue the ABS must overcome when it wants to use other agencies' data. In some cases, agencies have amended their legislation to facilitate this. Regardless of the arrangements put in place, once data is received by the ABS, it is subject to ABS secrecy provisions.<sup>77</sup>

3.67 Liberty Victoria added a warning that data matching, while 'an invaluable tool', is sometimes 'poorly handled' and carries the risk of inadvertent disclosure:

Liberty Victoria believes that data matching should only occur after thorough risk and cost/benefit analyses have been done. Moreover, where data from two or more classes is combined, the highest classification standard should apply. If implemented correctly, data matching and secrecy provisions should work together to ensure only necessary data matching is undertaken with appropriate safeguards.<sup>78</sup>

3.68 During the secrecy phone-in, the ALRC also received a number of calls on behalf of charity groups seeking, for example, to assist people wishing to trace their family, to become reconciled with family members, or to locate missing persons. In particular, concern was expressed about an inability to gain access to information that would assist them in such tasks.<sup>79</sup> While these are matters concerning privacy issues, rather than strictly ones concerning secrecy provisions, the callers said that the information held by agencies could assist in achieving the desired outcomes.

#### ***Secrecy provisions not inhibiting information sharing***

3.69 A number of investigative and law enforcement agencies expressed the view that their secrecy provisions generally did not unduly inhibit the sharing of information with respect to their operations where such sharing was necessary.<sup>80</sup> In this context, specific provisions and practices were designed to facilitate information sharing. The Australian Intelligence Community (AIC), for example, submitted that

current laws do not inhibit appropriate information sharing within the AIC and among AIC and relevant non-AIC agencies. For example, sections 6(1)(b), 6B(d), 7(b), 39, 39A, 40 & 41 of the *Intelligence Services Act [2001]* (Cth) specifically enable appropriate information sharing for [the Australian Secret Intelligence Service], [the

---

<sup>77</sup> Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

<sup>78</sup> Liberty Victoria, *Submission SR 19*, 18 February 2009.

<sup>79</sup> *Secrecy Phone-In*, 11–12 February 2009.

<sup>80</sup> Australian Intelligence Community, *Submission SR 37*, 6 March 2009; Australian Federal Police, *Submission SR 33*, 3 March 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

Defence Signals Directorate] and [the Defence Imagery and Geospatial Organisation]. Within the operation of these laws, persons with a ‘need to know’ may be appropriately security cleared to allow their receipt of national security-classified information. Where necessary, information can also be sanitised to a lower national security classification to allow the information to be shared more widely.

While subsection 18(2) of the [*Australian Security Intelligence Organisation Act 1979* (Cth) (*ASIO Act*)] creates a limited offence for unauthorised communication of any information a person has acquired by reason of being an officer or contractor of ASIO, the *ASIO Act* also identifies the circumstances in which information may be disseminated to other organisations and persons (see sections 17(1)(b), 18(3)(a) and (b), and 19(2)). Accordingly, provided it is done by officers acting within the limits of the authority conferred upon them by the Director-General or with the approval of the Director-General, ASIO will seek to communicate intelligence in support of its statutory obligations.<sup>81</sup>

3.70 The AFP also submitted that sharing information other agencies, including members of the AIC, was facilitated by a variety of instruments and laws:

The sharing and subsequent use of information is regulated by inter-agency Memorandums of Understanding (MOU), AFP Guidelines and legislative provisions depending on the type, context and classification of the information. The AFP holds that any reforms to Commonwealth secrecy provisions should not prevent, hinder or restrict this current ability to access and/or share information.<sup>82</sup>

3.71 However, the AFP wanted to ensure that

any reforms maintain or strengthen the strict provisions already in place so as to support the existing high degree of confidence our organisation presently enjoys within Government and the Australian Intelligence Community.<sup>83</sup>

3.72 In its submission, AUSTRAC commented that specific provisions relevant to its operations enabled information sharing:

Where the sharing of information concerns the primary disclosure between AUSTRAC and designated agencies, AUSTRAC considers that the secrecy provisions of the AML/CTF Act provide an appropriate balance between protecting and sharing AUSTRAC information. ... AUSTRAC considers that the AML/CTF Act secrecy provisions provide considerable flexibility in respect of secondary disclosure by designated agencies.<sup>84</sup>

3.73 In particular, AUSTRAC stated that the secrecy provisions of the AML/CTF Act facilitate international exchange of information:

The broad principles regarding international exchange of information between FIUs, including its further disclosure, are set out in the MOU between the 8 parties. These MOUs reflect the requirements set out in section 132(1) of the AML/CTF Act for such disclosures by AUSTRAC. As these MOUs are not enforceable, the secrecy

---

<sup>81</sup> Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

<sup>82</sup> Australian Federal Police, *Submission SR 33*, 3 March 2009.

<sup>83</sup> Ibid.

<sup>84</sup> Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

provisions of the AML/CTF Act provide reassurance and certainty to [foreign intelligence units] that information provided to AUSTRAC will not be disclosed except in specified circumstances, and vice versa.

The secrecy provisions of Division 4 of Part 11 of the AML/CTF Act enable the AFP, the ACC, ASIO and ASIS to communicate AUSTRAC information to a foreign government if satisfied that the foreign country will protect the confidentiality of the information, control its use and use it only for the purpose that it was provided.

3.74 However, AUSTRAC noted that where agencies are not designated under the AML/CTF Act, they

must seek legislative amendment to enable any comprehensive sharing of information, even though their role and function may fall within activities that could be otherwise or have previously been considered as relevant to the overarching objectives of the Act.<sup>85</sup>

3.75 Further, ASIC explained how information sharing is facilitated by s 127 of the *Australian Securities and Investments Commission Act 2001* (Cth) (ASIC Act):

The need for ASIC to release confidential information to either domestic law enforcement agencies or foreign regulators is increasing significantly.

ASIC releases information to both state and federal agencies and foreign regulators pursuant to s127 of the ASIC Act.

Section 127 sets out secrecy obligations for ASIC, and the circumstances where disclosure is authorised. Overlaying this is the common law obligation to provide procedural fairness to persons whose interests may be adversely affected by decisions made under this provision—*Johns v ASC* (1993) 178 CLR 408. Since the decision in *Johns*, ASIC has taken particular care to ensure that procedural fairness obligations are complied with.<sup>86</sup>

3.76 In the experience of the Australian Prudential Regulation Authority (APRA), the secrecy provision that applies to that agency has not limited its ability to share information with other agencies or the private sector nor has it inhibited them from sharing information about a regulated entity with that entity. APRA noted that the applicable secrecy provision contains a number of exceptions which allows them to disclose information to a ‘financial sector supervisory agency’ or a prescribed agency.<sup>87</sup>

3.77 The Department of Human Services (DHS) also remarked that it was able to match data successfully by entering into MOUs with other agencies.<sup>88</sup> The DHS noted,

---

85 Ibid.

86 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

87 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

88 Department of Human Services, *Submission SR 26*, 20 February 2009.

however, examples from its portfolio ‘where the restriction on sharing information could be further considered’:

- while Medicare Australia is able to disclose information to the police under a public interest certificate, often the police are unable to then share that information directly with prosecuting authorities and the courts. While practical workarounds are sometimes used (such as Medicare, rather than the police, making the further disclosures) the policy justification for this type of restriction could be questioned;
- [Commonwealth Rehabilitation Service (CRS)] Australia’s provisions do not deal explicitly with situations where the disclosure of information might assist in a criminal investigation, or where disclosure is necessary to protect against an imminent threat to a person’s life or physical safety. Currently, disclosures must be made under a public interest certificate executed by a delegate within the Department of Education, Employment and Workplace Relations. Timeliness is an issue; for example, when a person departs CRS Australia premises having threatened suicide or imminent physical harm to another, including employees at a place they are about to visit, the current secrecy provision prevents CRS Australia from taking protective action until a [Department of Education, Employment and Workplace Relations] delegate approves the disclosure; and
- Centrelink’s provisions tightly restrict its use of information within its customer database. For example, using its database to identify customers who might qualify for State Government benefits or non-government organisation services, and notifying them of those services, can be a problem as the secrecy provisions do not include authorisation for consent-based uses. This inhibits the capacity for Centrelink to operate in partnership with such organisations where doing so would clearly be to the benefit of the person concerned.<sup>89</sup>

### *Achieving the right balance*

3.78 Maintaining strict secrecy provisions is seen to support information sharing but at the same time provides protection to information in appropriate circumstances. The AGD suggested that:

robust and effective secrecy laws that enable information sharing while also protecting information from unauthorised disclosure at any point in the ‘distribution chain’ could enhance information sharing.<sup>90</sup>

3.79 The importance of ‘robust controls’ was echoed by AUSTRAC, who stated that the ability to share information is critical to its operations and that current guidelines provided a good framework for meeting privacy concerns:

AUSTRAC’s ability to combat money laundering and terrorism financing depends upon receiving and sharing information with a wide variety of designated agencies. Moreover, the ability to cross reference various sets of data supplied has proved to

---

89 Ibid.

90 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

significantly enrich the value of AUSTRAC financial intelligence and its contribution to operational success for AUSTRAC and designated agencies.

Bulk data matching can have significant benefits. However, it is crucial that any data matching exercise that involves AUSTRAC information be handled securely with robust controls and procedures in place that require compliance by all involved. All data matching exercises are carried out in accordance with the advisory Guidelines for the Use of Data-Matching in Commonwealth Administration issued by the Privacy Commissioner.<sup>91</sup>

3.80 The DHS noted in its submission that while secrecy provisions do inhibit the sharing of information, they are ‘designed to do so’. DHS pointed out that ‘whether the inhibition is inappropriate imports a value judgment on which the person concerned, the possessing agency and the requestor may well have divergent opinions’. Having listed the examples, set out above, where information sharing has been unnecessarily inhibited by secrecy provisions, the Department noted the challenge in ensuring that a secrecy provision strikes the appropriate balance:

It is a significant challenge to design a secrecy provision that adequately protects against unjustifiable dealings with sensitive information whilst retaining the capacity for agencies to use and disclose that information in proper circumstances and for proper purposes. Part of the challenge is in determining whose judgment is to be preferred in striking the balance. At present, secrecy laws are a mixture of the legislature, the Minister in the administering agency or a senior officer (by way of public interest certificates or similar instruments), and the person whose information is concerned (i.e. a consent based system).<sup>92</sup>

3.81 DHS regarded this as ‘an issue across government’ and described it as a ‘conundrum’.<sup>93</sup>

3.82 The Department of Climate Change identified drafting as a critical issue in achieving the right balance between protecting and sharing information:

There is a potential risk that federal secrecy provisions may inhibit sharing of information between law enforcement agencies, governments and between governments and the private sector. It is important that secrecy provisions be drafted with sufficient flexibility to ensure that persons with legitimate uses for information are able to access it, whilst protecting valuable information from misuse and ensuring only persons with a genuine need to know receive such information.<sup>94</sup>

#### ***Agency head authorisation***

3.83 In terms of how best to balance the need to share information between agencies, while also ensuring accountability for the protection of the information, the AGD

---

91 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

92 Department of Human Services, *Submission SR 26*, 20 February 2009.

93 Ibid.

94 Department of Climate Change, *Submission SR 27*, 23 February 2009.

suggested that a general secrecy provision allow the agency head or a senior officer to authorise disclosure:

Including a provision to enable the agency head or other senior officers to authorise disclosure may provide greater flexibility as it may enable disclosure in new or unforeseen circumstances. It also provides a level of accountability by requiring a senior officer to consider whether disclosure would be consistent with policy considerations in a particular case. Memorandums of understanding (MOU) or internal guidelines may also be used to set out circumstances when information can be disclosed from one agency to another. This may provide a more flexible approach, as the detail of information sharing arrangements can be left to documents more easily amended.<sup>95</sup>

3.84 The Department of Education, Employment and Workplace Relations discussed the need for information sharing where a whole of government or cross-portfolio response is needed to deliver Government initiatives, but also expressed reservations about the ‘agency head’ approach in practice:

[T]here are increasingly a number of Government initiatives which cut across the portfolio responsibility of a number of Commonwealth agencies. The ability to deliver good outcomes for these initiatives is often reliant upon a whole of government response and thus necessitates the sharing of information between relevant Commonwealth agencies and community organisations. However, agency specific provisions can often pose a barrier to getting policy measures, aimed at benefiting the community, up and running. For example, the confidentiality provisions in the social security and family assistance law authorise the use and disclosure of protected information in a number of prescribed circumstances. These circumstances however in the main tend to be tied back to purposes which are linked to or benefit a social security or family assistance outcome. Accordingly, the Department would be very limited, if not prevented, from using and disclosing protected information for the purposes of a policy initiative which was aimed at assisting vulnerable members of the community, where that initiative did not serve a social security or family assistance law purpose or could be tied back to a matter of direct relevance to this Department.

While exceptions such as consent or some sort of head to head power which authorises the head of a Department of State of the Commonwealth to disclose protected information to the head of another Commonwealth authority are available, they are generally not practicable in the above type of scenario.<sup>96</sup>

### ***Culture***

3.85 The AGD referred to a number of reports that have considered the impact of secrecy laws on information sharing<sup>97</sup> and suggested that:

---

95 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

96 Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

97 P Ford, *Report of the Review of Information and Intelligence Sharing in the Aviation Sector* (2006); Australian Federal Police National Security Operations Review Committee, *The Street Review: A Review of Interoperability Between the AFP and its National Security Partners* (2008); R Smith, *Review of Homeland and Border Security* (2008).

while there are some legislative barriers, a greater barrier to information sharing has tended to relate to cultures of secrecy within some of the relevant agencies. This seems to reflect the tension between the ‘need to know’ principle and the ‘need to share’ principle.<sup>98</sup>

3.86 Whistleblowers Australia and Australia’s Right To Know (ARTK) coalition also identified a cultural issue, the former commenting that:

There is a strong cultural issue driving public sector agencies to protect information for no reason other than they claim it as their own. No matter how banal a piece of information or a document may be, agencies tend to guard it as though it is a redraft of the Magna Carta.<sup>99</sup>

3.87 The ARTK coalition argued that the solution lay in a fundamental change in approach to government information:

Such sharing would be facilitated not by developing integration policies for information but by adopting a fundamentally more open approach to public information held in trust by Government.<sup>100</sup>

### **ALRC’s views**

3.88 If it is true that most individuals would prefer not to have to be repeatedly asked for the same information, there is also a general understanding that individuals who provide information to government agencies do so for a specific purpose and are entitled to a level of protection of that information. Where information is to be shared, people should know about it.

Australians rightly demand the delivery of government programs and services in a seamless way. They should also expect that, behind the scenes, all the resources of government will be brought to bear in the search for innovative solutions to the complex challenges of developing public policy.<sup>101</sup>

3.89 The Privacy Principles provide an appropriate framework for the management of personal information at an agency level. The PSM provides a framework for the classification of information broadly for the purposes of national security.

3.90 The ALRC considers that, as a general principle, information sharing between government agencies, and government and the private sector, is best undertaken at the agency level through individual agency agreements.<sup>102</sup> Such agreements, however,

---

98 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

99 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

100 Australia’s Right to Know, *Submission SR 35*, 6 March 2009.

101 Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia’s Priority Challenges* (2004), Preface, Dr Peter Shergold.

102 Agency information-handling policies and MOUs are discussed in Ch 15.

need to sit within the framework of information management, including any applicable secrecy provisions.

3.91 The new general secrecy offence proposed by the ALRC—discussed in Chapters 7, 8 and 9—proposes an exception to the offence where the disclosure is authorised by the relevant agency head or minister, which would potentially cover information disclosed in accordance with information sharing agreements or agency information-handling policies.<sup>103</sup> In some circumstances, however, it may be considered desirable to set out in legislation the circumstances in which information sharing is permissible, such as in the case of intelligence information or in the anti-money laundering context. Chapter 11 considers this issue further in the context of the codification of permissible disclosures in specific secrecy provisions.

---

103      Proposal 9–1.

## **4. Freedom of Information, Privacy and Secrecy**

---

### **Contents**

Introduction	105
Freedom of information	106
Overview of the <i>Freedom of Information Act 1982</i> (Cth)	106
Exemptions	107
Assessing the public interest	113
The interaction between FOI and secrecy	117
An appropriate balance between secrecy and open government?	123
Submissions	124
ALRC's views	131
Archives	134
Overview of the <i>Archives Act 1983</i> (Cth)	134
Exemptions	135
Secrecy and the <i>Archives Act</i>	136
Submissions	138
ALRC's views	140
Privacy	143
Overview of the <i>Privacy Act 1988</i> (Cth)	143
Privacy and secrecy	145
Submissions	148
ALRC's views	151

### **Introduction**

4.1 In this chapter, the Australian Law Reform Commission (ALRC) considers the relationship between Commonwealth secrecy laws and other Commonwealth laws dealing with the handling of information. As Associate Professor Moira Paterson remarked in her treatise on *Freedom of Information and Privacy in Australia*, there is a

complex tapestry of interconnected and overlapping statutory regimes that govern access to, and amendment of, government information, including freedom of

information laws, privacy laws (including information privacy and health records laws) and public records laws.<sup>1</sup>

4.2 The principal components of the overlapping regimes at the Commonwealth level are the *Freedom of Information Act 1982* (Cth) (FOI Act), the *Archives Act 1983* (Cth) and the *Privacy Act 1988* (Cth). Each will be considered in turn.

## **Freedom of information**

### **Overview of the *Freedom of Information Act 1982* (Cth)**

4.3 The FOI Act provides a right of access to information held by government agencies and ministers. Access is provided both through an obligation to publish certain information<sup>2</sup> as well as a right to apply for the production of documents.<sup>3</sup> The FOI Act also gives a person a right to annotate or correct personal records held by government agencies.<sup>4</sup> Hence there are two broad types of information covered: official information; and personal information.

4.4 However, the principle of open government, which a right of access enshrines, has to be balanced with the practical need of a government to be able to govern and, for that purpose, to be able to keep some documents protected from disclosure. This is expressed in the FOI Act by the exemption provisions, the purpose of which is ‘to balance the objective of providing access to government information against legitimate claims for protection’.<sup>5</sup> As stated in the current objects clause, the exemptions are those

necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by departments and public authorities.<sup>6</sup>

4.5 The FOI Act is currently the subject of an Exposure Draft of the Freedom of Information Amendment (Reform) Bill 2009 (FOI Exposure Draft Bill), containing a number of key amendments to implement the election policy commitments of the current Labor Government in this area.<sup>7</sup>

4.6 This chapter considers the present workings of the FOI Act, the proposed amendments in the FOI Exposure Draft Bill, as well as proposals for the purposes of this Inquiry arising in response to matters raised in the Issues Paper, *Review of Secrecy Laws* (IP 34).

1 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [1.2].

2 *Freedom of Information Act 1982* (Cth) pt II.

3 *Ibid* pt III.

4 *Ibid* pt V.

5 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [8.1].

6 *Freedom of Information Act 1982* (Cth) s 3(1)(b).

7 K Rudd and J Ludwig, *Government Information: Restoring Trust and Integrity—Election 2007 Policy Document* (2007) Australian Labor.

## Exemptions

4.7 A document may be exempt from the operation of the FOI Act if an agency or body is exempt; if the document is an exempt document under Part IV of the Act; or it is an official document of a Minister that contains some matter that does not relate to the affairs of an agency or of a Department of State.<sup>8</sup>

4.8 Notwithstanding that a document may fall within an exempt category, there may nevertheless be a requirement, where practicable, to provide an applicant with access to an edited copy from which any exempt matter has been deleted.<sup>9</sup> Moreover, s 14 provides that:

Nothing in this Act is intended to prevent or discourage Ministers and agencies from publishing or giving access to documents (including exempt documents), otherwise than as required by this Act, where they can properly do so or are required by law to do so.

4.9 The FOI Exposure Draft Bill will, if implemented, have a significant impact on the way the exemption provisions are presently cast. These are considered below.

### *Exemptions for certain agencies and documents*

4.10 Section 7 of the FOI Act provides a complete exemption for documents that have originated with, or been received from, certain agencies, including the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), the Office of National Assessments (ONA), the Inspector-General of Intelligence and Security (IGIS) and the Defence Imagery and Geospatial Organisation (DIGO).

4.11 Other Commonwealth agencies that handle a significant amount of material relating to national security, such as the Department of Foreign Affairs and Trade, the Department of Immigration and Citizenship, and the Australian Federal Police, are open to FOI applications. However, s 7(2A) provides an exemption for all agencies in relation to documents that originate with, or have been received from, ASIS, ASIO, ONA, DIGO, the Defence Intelligence Organisation, the Defence Signals Directorate or the IGIS.

4.12 The proposed amendments to the FOI Act included in the FOI Exposure Draft Bill leave largely untouched the exempt agency aspects of the existing Act, hence, as noted by Cabinet Secretary, Senator the Hon John Faulkner:

That exclusion is maintained, and in some areas clarified, such as to cover extracts from such documents.

---

8 *Freedom of Information Act 1982* (Cth) s 4(1) definition of ‘exempt document’. The FOI Exposure Draft Bill proposes no change to the definition of ‘exempt document’.

9 *Ibid* s 22. The FOI Exposure Draft Bill cl 14 proposes a rewording of this section.

The Defence Department will be excluded for documents in respect of its collection, reporting and analysis of operational intelligence and special access programs under which a foreign government provided restricted access to technologies.

I make no apology for these exclusions.

There is a strong, in my view undeniable, public interest argument why this information ought to be protected. National security is a fundamental responsibility of Government.

Classified national security information must be protected by the government in the national interest. This is right, it is vital, and it is not going to change.

I just want to make it very clear, so everyone understands, what information the Government believes we have a responsibility to keep *out* of the public area.

These are clear—and *limited*—exceptions to the general principle of disclosure.<sup>10</sup>

4.13 There are, however, proposals for significant amendment of the exemptions under pt IV of the existing FOI Act. The present form of the pt IV exemptions will be considered first, followed by the amendments proposed by the FOI Exposure Draft Bill.

#### ***Exemptions under Part IV***

4.14 Access to documents may be denied on the basis of one of the specific grounds of exemption under pt IV of the FOI Act. These exemptions presently include: documents affecting national security, defence or international relations;<sup>11</sup> Cabinet documents;<sup>12</sup> internal working documents;<sup>13</sup> documents relating to business affairs;<sup>14</sup> and documents affecting the national economy.<sup>15</sup>

4.15 The exemptions in pt IV can be analysed as falling into two broad categories: class-based exemptions; and exemptions that depend on demonstrating the expected harm that would be caused by disclosure.

#### ***Class-based exemptions***

4.16 In this group of exemptions, documents are exempt by virtue of their nature, for example, a ‘Cabinet document’.<sup>16</sup> Other exemptions in this category are for Executive Council documents;<sup>17</sup> where secrecy provisions or legal professional privilege apply,

---

10 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

11 *Freedom of Information Act 1982* (Cth) s 33.

12 Ibid s 34.

13 Ibid s 36.

14 Ibid s 43.

15 Ibid s 44.

16 If it meets the definition of Cabinet document in s 34(1).

17 *Freedom of Information Act 1982* (Cth) s 35.

or where disclosure would be in contempt of Parliament or contempt of court;<sup>18</sup> for electoral rolls;<sup>19</sup> and under companies and securities legislation.<sup>20</sup>

4.17 The exemption for Cabinet documents is the clearest expression of the interaction between open government ideas and the concept of Westminster government, in its emphasis on the need for confidentiality of the collective Cabinet decision-making process. In this case, it has been said that disclosure would cause greater harm to the public interest than the withholding of any documents.<sup>21</sup> It does not matter that the consequences of disclosure may be infinitesimal; the harm comes from the inherent shattering of Cabinet security.

4.18 The operation of class-based exemptions is one of strict principle. There is no additional assessment of the merits for and against disclosure, or harm caused, only that the document satisfies the particular categorisation within the section. To the extent that there is a notion of public interest it may be said to be implicit, namely that there is already a judgment that it would not be in the public interest for documents in these categories to be amenable to access under the FOI Act. The extent to which this continues to be appropriate is the subject of the FOI Exposure Draft Bill and surrounding material—as well as this Inquiry, with respect to secrecy provisions.

4.19 The FOI Exposure Draft Bill proposes the reduction of the number of class-based exemptions and a recasting of some others, such as the Cabinet exemption. In particular, the latter exemption is reformulated to limit it to the documents ‘at the core of the Cabinet process’, as explained in the *Freedom of Information (FOI Reform) Companion Guide (Companion Guide)*, released with the Bill:

The current Cabinet exemption protects submissions that have gone, or are proposed to go, to the Cabinet, as well as official Cabinet records and documents that would disclose any Cabinet deliberation or decision. The proposed Cabinet exemption is more specific, and covers:

- Cabinet submissions and proposed submissions that meet the ‘dominant purpose’ test (even if never submitted to Cabinet);
- official records of Cabinet;
- briefing notes created for the dominant purpose of briefing a Minister on Cabinet submissions or proposed submissions;
- drafts, copies or extracts of such documents; and
- a document, to the extent that it would reveal a Cabinet deliberation or decision (unless already published).<sup>22</sup>

18 Ibid ss 38, 42, 46.

19 Ibid s 47A.

20 Ibid s 47.

21 *Whitlam v Australian Consolidated Press* (1985) 60 ACTR 7, 15–16.

22 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009).

4.20 It is also proposed that a number of class-based exemptions be repealed. As recommended by the ALRC and the Administrative Review Council (ARC) in 1995, *Open Government: A Review of the Federal Freedom of Information Act 1982* (ALRC 77), the FOI Exposure Draft Bill proposes the repeal of the exemptions for Executive Council documents; documents arising out of companies and securities legislation; and documents relating to the conduct of an agency of industrial relations.<sup>23</sup>

4.21 However, there is no proposal in the FOI Exposure Draft Bill with respect to the secrecy exemption in s 38 of the FOI Act. This exemption is considered expressly later in this chapter, after a consideration of the other broad category of exemptions, namely those based on anticipated harm.

#### ***Anticipated harm based exemptions***

4.22 This category of exemptions depends on demonstrating the expected harm that would be caused by disclosure. For example, documents ‘affecting national security, defence or international relations’ are exempt under the present form of s 33(1) if disclosure:

- (a) would, or could reasonably be expected to, cause damage to:
  - (i) the security of the Commonwealth;
  - (ii) the defence of the Commonwealth; or
  - (iii) the international relations of the Commonwealth; or
- (b) would divulge any information or matter communicated in confidence by or on behalf of a foreign government, an authority of a foreign government or an international organization to the Government of the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth or of an authority of the Commonwealth.

4.23 Other exemptions in this category presently include: Commonwealth-State relations;<sup>24</sup> law enforcement and public safety;<sup>25</sup> the financial or property interests of the Commonwealth;<sup>26</sup> operations of agencies;<sup>27</sup> business and professional affairs;<sup>28</sup> research;<sup>29</sup> the national economy;<sup>30</sup> and material obtained in confidence.<sup>31</sup> The document is exempt provided that its disclosure would result in harm of the kind identified. With respect to the personal privacy exemption, the harm is expressed in

---

23 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

24 *Freedom of Information Act 1982* (Cth) s 33A.

25 Ibid s 37.

26 Ibid s 39.

27 Ibid s 40.

28 Ibid s 43.

29 Ibid s 43A.

30 Ibid s 44.

31 Ibid s 45.

terms of whether disclosure would be ‘unreasonable’ in the circumstances.<sup>32</sup> The business affairs exemption also includes a similar requirement that disclosure ‘would, or could reasonably be expected to, unreasonably affect’ the relevant person adversely in the circumstances stated.<sup>33</sup>

4.24 In each case the harm may be seen to reflect an identified, or essential,<sup>34</sup> public interest, whether it is the security of the Commonwealth, or security of personal information.

4.25 In the internal working documents exemption, the harm is expressed more abstractly, in terms of being contrary to the public interest.<sup>35</sup> Under s 36 a document is exempt if its disclosure:

- (a) would disclose matter in the nature of, or relating to, opinion, advice or recommendation obtained, prepared or recorded, or consultation or deliberation that has taken place, in the course of, or for the purposes of, the deliberative processes involved in the functions of an agency or Minister or of the Government of the Commonwealth; and
- (b) would be contrary to the public interest.

4.26 The FOI Exposure Draft Bill proposes a number of reforms to the anticipated harm exemptions. These are considered below.

### ***Proposed reforms***

4.27 Two main features of the reforms proposed in ALRC 77, in the Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 and the FOI Exposure Draft Bill, are the abolition of ‘conclusive certificates’ and the integration of public interest elements in a variety of ways.

### ***Conclusive certificates***

4.28 A ‘conclusive certificate’ is one issued by the minister responsible for an agency and has the effect of making the document the subject of the certificate exempt for as long as the certificate remains in force and operates, as described in ALRC 77, as a ‘ministerial veto’.<sup>36</sup> In the current FOI Act there are veto provisions of this nature in several sections.<sup>37</sup>

---

32 Ibid s 41.

33 Ibid s 43.

34 To use the language of the objects clause: Ibid s 3(1)(b).

35 Ibid s 36.

36 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [8.17].

37 *Freedom of Information Act 1982* (Cth) s 33 (documents affecting national security, defence or international relations); 33A (documents affecting relations with states); s 34 (Cabinet documents); s 35 (Executive Council documents); and s 36 (internal working documents).

4.29 In 1995, in ALRC 77, the ALRC and ARC recommended the abolition of conclusive certificates in most cases, retaining them only in two contexts: national security and defence; and Cabinet documents.<sup>38</sup> Amendments to the FOI Act now under consideration will, if enacted, go further.

4.30 As the first step in implementing its election commitments regarding FOI reform,<sup>39</sup> the government has introduced the Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008. The primary purpose of this Bill is to remove the power to issue conclusive certificates under both the FOI Act and the *Archives Act*.<sup>40</sup>

#### ***Public interest test***

4.31 In ALRC 77, the importance of a public interest requirement in determining whether material should be exempt from disclosure was reiterated:

Public interest tests allow all considerations relevant to a particular request to be balanced. They are therefore an important and necessary feature of the [FOI Act], even though it can at times be difficult to perform this balancing exercise.<sup>41</sup>

4.32 The ALRC also recommended that the proposed Information Commissioner should issue guidelines on how to apply such a test and that, for the purpose of determining whether the release of a document would be contrary to the public interest, it should be irrelevant that the disclosure ‘may cause embarrassment to the government’.<sup>42</sup>

4.33 At the time, however, the idea of a general exemption—that the disclosure of the document in question ‘would be contrary to the public interest’—was not considered appropriate, on the basis that it would be ‘uncertain and vulnerable to idiosyncratic decision making’.<sup>43</sup>

4.34 Since then, however, there has been increasing pressure on such exemptions in the interests of public accountability of government decision making. In consequence, on 24 March 2009, Senator Faulkner announced significant amendments to the exemption provisions of the FOI Act. In addition to amending the Cabinet exemption and repealing particular class-based exemptions, noted above, many existing

38 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [8.17].

39 K Rudd and J Ludwig, *Government Information: Restoring Trust and Integrity—Election 2007 Policy Document* (2007) Australian Labor.

40 See Explanatory Memorandum, Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth).

41 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [8.1].

42 Ibid, Recs 37–38.

43 Ibid, [8.6]. The possibility had been raised in the Issues Paper which preceded the Report, but was ‘overwhelmingly rejected in submissions’: fn 15.

exemptions are to be made subject to a public interest test, and referred to as ‘conditional exemptions’. As Senator Faulkner explained:

The draft legislation divides exemptions into those which are subject to a public interest test (called conditional exemptions) and those that are not, and then applies a single simple, strong and clear test to all conditional exemptions, which requires an agency to give access to a document unless giving that access would at the time, ‘on balance, be contrary to the public interest’.<sup>44</sup>

4.35 Of the existing anticipated harm exemptions, those concerning personal privacy,<sup>45</sup> business affairs,<sup>46</sup> the national economy<sup>47</sup> and research,<sup>48</sup> will all be brought under the umbrella of the conditional exemption category, with a common public interest test.<sup>49</sup>

4.36 This proposal is similar to the approach recommended in Queensland in June 2008 by the Independent Review Panel examining the *Freedom of Information Act 1992* (Qld)—chaired by Dr David Solomon (the Solomon Committee)—that a single public interest test be included in that Act:

Access is to be provided to matter unless its disclosure, on balance, would be contrary to the public interest.<sup>50</sup>

4.37 The effect of the proposed amendments is not, however, to introduce a ‘single exemption’ in the Commonwealth legislation; rather, as noted by Peter Timmins:

Exemptions will now be arranged in two neat boxes—absolute exemptions, and conditional exempt documents where a public interest test applies.

Some media reports suggest confusion that the Minister’s statement about a single public interest test means there will be one exemption. That’s what Queensland is proposing. Federally it means only that the current situation of several different formulations of a public interest test in the Act will be replaced by one test—whether disclosure is contrary to the public interest, relevant only to specified exemptions but not others.<sup>51</sup>

## Assessing the public interest

4.38 Throughout the FOI Act and discussions of reforming it lie threads of ideas about public interest. Here, too, the same multiple uses of the phrase ‘public interest’

44 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

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

46 Ibid s 43.

47 Ibid s 44.

48 Ibid s 43A.

49 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

50 Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), Rec 41.

51 P Timmins, *Some analysis of the FOI reform package* (2009) <<http://www.foi-privacy.blogspot.com/>> at 30 March 2009.

referred to in Chapter 2 are evident. There is the identification in the current objects clause that the exemptions of the FOI Act are aimed at protecting ‘essential public interests’.<sup>52</sup> There is also the notion of ‘the public interest’, which is used, for example, in s 36, where being ‘contrary to the public interest’ is an element of the exemption; and in s 40, where the particular exemption does not apply if disclosure ‘would, on balance, be in the public interest’. Ideas of public interest therefore provide a backdrop for, or are integrated in various ways into, the legislation and particular aspects of it.

4.39 In *McKinnon v Secretary, Department of Treasury*,<sup>53</sup> the High Court had occasion to comment on the public interest element in s 36 of the FOI Act. Michael McKinnon had applied for access to government documents concerning, amongst other things, the first home owners scheme administered by the Department of Treasury. The request for access to many of the documents was rejected on the basis that their release would be contrary to the public interest and the Treasurer signed a certificate to that effect. The litigation tested the ability to review the conclusive certificate. The Administrative Appeals Tribunal determined that reasonable grounds existed for the claims and the High Court agreed, dismissing the appeal. While the amendments to the FOI Act under consideration will, if enacted, repeal the power to issue conclusive certificates and make exemption decisions subject to full merits review,<sup>54</sup> the comments about the concept of public interest made by the court remain pertinent. For example, Gleeson CJ and Kirby J commented that a judgment ‘as to where the public interest lies’

is not made in a normative vacuum. It is made in the context of, and for the purposes of, legislation which ... begins from the premise of a public right of access to official documents, and which acknowledges a qualification of that right in the case of necessity for the protection of *essential* public interests.<sup>55</sup>

4.40 The multi-dimensional, or multi-faceted nature of public interest was also remarked upon by Hayne J:

It may readily be accepted that most questions about what is in ‘the public interest’ will require consideration of a number of competing arguments about, or features or ‘facets’ of, the public interest. As was pointed out in *O’Sullivan v Farrer* [(1989) 168 CLR 210, 216]:

[T]he expression ‘in the public interest’, when used in a statute, classically imports a discretionary value judgment to be made by reference to undefined factual matters, confined only ‘in so far as the subject matter and the scope and purpose of the statutory enactments may enable ... given reasons to be [pronounced] definitely extraneous to any objects the legislature could have had in view’.

52 Freedom of Information Act 1982 (Cth) s 3(1)(b).

53 *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423.

54 Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth); Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft; and see Explanatory Memorandum, Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth) and J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009).

55 *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, [5].

That is why a question about ‘the public interest’ will seldom be properly seen as having only one dimension.<sup>56</sup>

### ***Defining the public interest***

4.41 When considering the Bill that led to the FOI Act, the Senate Committee on Constitutional and Legal Affairs referred to public interest as a

phrase that does not need to be, indeed could not usefully, be defined ... Yet it is a useful concept because it provides a balancing test by which any number of relevant interests may be weighed one against another ... the relevant public interest factors may vary from case to case—or in the oft quoted dictum of Lord Hailsham of Marylebone ‘the categories of the public interest are not closed’.<sup>57</sup>

4.42 While not attempting to define public interest, to assist in interpreting the public interest test proposed in the FOI Exposure Draft Bill, two lists of factors to be considered are included: one of factors that point towards disclosure, the other of those that are irrelevant.

4.43 The ‘non-exhaustive’ list of factors to be weighed *in favour* of disclosure are those that disclosure would:

- (a) promote the objects of [the] Act ... ;
- (b) inform debate on a matter of public importance;
- (c) promote effective oversight of public expenditure;
- (d) allow a person to access his or her own personal information.<sup>58</sup>

4.44 In assessing whether access would, on balance, be contrary to the public interest, the following factors must not be taken into account:

- (a) access to the document could result in embarrassment to the Commonwealth Government, or cause a loss of confidence in the Commonwealth Government;
- (b) access to the document could result in the applicant misinterpreting or misunderstanding the document;
- (c) the author of the document was (or is) of high seniority in the agency to which the request for access to the document was made;
- (d) access to the document could result in confusion or unnecessary debate.<sup>59</sup>

---

<sup>56</sup> Ibid, [55]. Compare, however, the comments of Callinan and Heydon JJ at [130].

<sup>57</sup> Australian Senate Committee on Constitutional and Legal Affairs, *Report on Draft Commonwealth Freedom of Information Bill* (1979), [5.28].

<sup>58</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, cl 11B(3).

<sup>59</sup> Ibid, cl 11B(4). A similar approach was recommended in Queensland: Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), 152–154, Rec 42.

4.45 Complementing these lists of factors is the proposal that an agency or minister must have regard to any guidelines issued by the proposed Information Commissioner.<sup>60</sup>

4.46 The list of factors favouring disclosure also emphasises the ‘cultural shift’ sought to be produced by the FOI Exposure Draft Bill, as explained by Senator Faulkner:

These reforms will change the law, but they also demonstrate the government’s commitment to culture change, a shift from the culture of secrecy ... to one of openness and transparency.<sup>61</sup>

### ***Comparative approaches to public interest***

4.47 The United Kingdom (UK) came late to FOI, in the *Freedom of Information Act 2000* (UK) (UK FOI Act). Similar to the Australian legislation, it includes two types of exemption—absolute or qualified. With respect to the latter, a balancing of public interests is required by assessing whether the public interest in maintaining the exclusion outweighs the public interest in disclosure.<sup>62</sup>

4.48 In contrast to Australia, there is no absolute exemption for Cabinet documents—rather, a balancing approach is required. In assessing whether Cabinet documents should, or should not, be released in response to an FOI request, the authority must balance the exclusion against the public interest in disclosure, taking into account public interest factors such as the promotion of government accountability. Provided the public interest is best served by disclosure rather than exclusion, the exemption will not apply.<sup>63</sup>

4.49 In a recent decision involving the disclosure of Cabinet minutes relating to the Iraq war, the Information Commissioner, the independent regulator of the UK FOI Act’s provisions, applied such a test. Considering the gravity and controversial nature of the subject matter, the desire for accountability and transparency in government decision making, and the role of public participation in such actions, the Commissioner disclosed the documents in February 2008, holding that these factors outweighed any possible harm that might emerge from disclosure. Although the Commissioner’s decision was upheld by the Information Tribunal,<sup>64</sup> the decision was subsequently

---

60 Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, cl 11B(5). See also the recommendation in Queensland: Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), Rec 43.

61 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

62 *Freedom of Information Act 2000* (UK) s 2(1)(b).

63 Information Commissioner’s Office (UK), *Freedom of Information Act Awareness Guidance No 24: Policy Formulation, Ministerial Communications, Law Officers’ Advice, and The Operation of Ministerial Private Office* (Version 2, 2008).

64 *Cabinet Office v Information Commissioner* (Unreported, Information Tribunal, 27 January 2009).

overridden by the Rt Hon Jack Straw, Lord Chancellor and Secretary of State for Justice,<sup>65</sup> a decision which attracted considerable criticism.<sup>66</sup>

4.50 The *Official Information Act 1982* (NZ) also includes a public interest element. Section 9 allows information disclosure if the reasons for withholding it are outweighed by other considerations which render it desirable to disclose the information in the public interest. The section then goes on to describe those reasons, which are similar but not identical to the exemption provisions set out in the current Australian FOI Act.

### The interaction between FOI and secrecy

4.51 The interaction between the FOI Act and secrecy laws is seen directly in the exemption of certain agencies from the operation of the legislation, both in Australia and comparative jurisdictions, and also where there is an express secrecy exemption. In the Australian legislation the secrecy exemption is found in s 38.

4.52 While the FOI Exposure Draft Bill and Companion Guide consider many of the exemptions in the existing FOI Act, there is no mention made of s 38.<sup>67</sup>

#### *The secrecy exemption*

4.53 The secrecy exemption provides that documents or information contained in documents that are subject to certain secrecy provisions, do not need to be disclosed under the FOI Act. Secrecy provisions in other enactments can therefore be invoked by a government agency or minister to refuse access to a document under the FOI regime.

4.54 The secrecy exemption may apply to documents or information if a secrecy provision prevents disclosure and is set out in sch 3 of the FOI Act;<sup>68</sup> or enlivens the secrecy exemption by expressly applying s 38 of the FOI Act.<sup>69</sup>

4.55 The secrecy exemption applies only to the extent that a secrecy provision prohibits disclosure to the person making the FOI request.<sup>70</sup> In addition, the secrecy exemption does not apply if the relevant document or information contains personal

---

65 Ministry of Justice, *Exercise of the Executive Override under Section 53 of the Freedom of Information Act 2000* (2009) <<http://www.justice.gov.uk/docs/foi-statement-reasons.pdf>> at 19 March 2009.

66 G Slapper, *Iraq Cabinet Minutes: 'Jack Straw Should Not Be His Own Judge'* (2009) TIMESONLINE <<http://business.timesonline.co.uk/tol/business/law/article5801842.ece>> at 25 February 2009. See also the Information Commissioner's statement in response: R Thomas, *Veto of the publication of minutes of key Cabinet meetings: Statement* Information Commissioner's Office (UK).

67 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009).

68 *Freedom of Information Act 1982* (Cth) s 38(1)(b)(i).

69 *Ibid* s 38(1)(b)(ii).

70 *Ibid* s 38(1A).

information that relates only to the person making the request,<sup>71</sup> and s 503A of the *Migration Act 1958* (Cth) does not apply.<sup>72</sup>

4.56 Finally, a person cannot be prosecuted under a secrecy provision if that person discloses a document that is the subject of a request under the FOI Act if the person is of ‘the bona fide belief that access was required’ by the Act.<sup>73</sup> Disclosure in ‘good faith’ in the absence of an FOI request does not, however, attract this protection under the current law.<sup>74</sup>

4.57 The secrecy exemption in the FOI Act was intended to preserve the operation of existing Commonwealth secrecy provisions. In its report on the Freedom of Information Bill 1978, the Senate Standing Committee on Legal and Constitutional Affairs expressed concern, however, about the wide ambit of the proposed secrecy exemption, and recommended that it should only apply to prescribed secrecy provisions contained in a schedule to the Bill.<sup>75</sup> Secondly, the Committee was of the view that ‘all criminal provisions prohibiting or restricting the disclosure of information that are not prescribed under the Bill should be repealed’.<sup>76</sup>

4.58 The Committee’s second recommendation was not taken up, and the first recommendation was not immediately implemented. Instead, a broadly worded secrecy exemption was contained in the FOI Act as enacted in 1982.<sup>77</sup> In 1991, however, the FOI Act was amended to include sch 3, as well as the requirement that secrecy provisions either be listed in this schedule, or expressly apply the secrecy exemption.<sup>78</sup> Section 38(1A) also makes it clear that a document may still be disclosed, notwithstanding the secrecy exemption, if disclosure in the circumstances is not prohibited.

---

71     *Re Richardson and Federal Commissioner of Taxation* (2004) 81 ALD 486, 503; *Petroulias v Commissioner of Taxation* [2006] AATA 333, [65]–[66].

72     Freedom of Information Act 1982 (Cth) s 38(2), (3). The *Migration Act 1958* (Cth) s 503A is discussed below.

73     Freedom of Information Act 1982 (Cth) s 92(1)(b). See also *Actors’ Equity v Australian Broadcasting Tribunal* (1984) 6 ALD 68, 80–81.

74     Compare cl 92 of Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft; and see Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 11.

75     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), Rec 21.13(a).

76     Ibid, Rec 21.13(c).

77     The original s 38 of the FOI Act provided that: A document is an exempt document if there is in force an enactment applying specifically to information of a kind contained in the document and prohibiting persons referred to in the enactment from disclosing information of that kind, whether the prohibition is absolute or is subject to exceptions or qualifications.

78     Freedom of Information Amendment Act 1991 (Cth) ss 28, 47.

4.59 A document is exempt ‘only to the extent that a complying secrecy provision prohibits its disclosure’.<sup>79</sup> So, for example, if disclosure is permitted in the course of a Commonwealth officer’s duties, this would not be in breach of the relevant secrecy provision. As Paterson points out:

Unless the reference to duties etc is constrained or limited in some way, it will encompass freedom of information disclosure as well as other routine disclosures.<sup>80</sup>

4.60 Currently, sch 3 contains over 50 provisions in 28 Acts and one sub-regulation. This list includes, for example, provisions of the *Australian Security Intelligence Organisation Act 1979* (Cth), *Intelligence Services Act 2001* (Cth), *Child Support (Assessment) Act 1989* (Cth) and *Designs Act 2003* (Cth).

4.61 Schedule 3 has been amended several times since its introduction. The provisions in 11 Acts have been removed entirely from the list,<sup>81</sup> provisions in nine new Acts added to the list,<sup>82</sup> and a number of provisions in remaining Acts amended.<sup>83</sup> In addition, since 1991, a number of provisions in other Acts have expressly applied s 38 of the FOI Act with respect to certain information.<sup>84</sup> Some of these provisions are also listed in sch 3;<sup>85</sup> others are not.<sup>86</sup>

4.62 In its terms, s 38(1)(b)(ii) seems to require that for a secrecy provision to be relied upon as a basis for exemption, it must either be listed expressly in sch 3 or expressly apply s 38 to the document or information for which exemption is claimed.<sup>87</sup> What if a secrecy provision is not listed in sch 3 and does not expressly apply the secrecy exemption in s 38?

4.63 This issue arose in the Federal Court decision of *Kwok v Minister for Immigration and Multicultural Affairs, (Kwok)*<sup>88</sup> in which Tamberlin J considered s 503A of the *Migration Act*, restricting the disclosure by Commonwealth officers of

79 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.97].

80 Ibid, [8.98].

81 Deletions from the original sch 3 include: *Wool Tax (Administration) Act 1964* (Cth) s 8(2), (5) (repealed) and *Social Security Act 1991* (Cth) ss 1312(1), 1336(2). Provisions in the *Designs Act 1906* (Cth) were replaced by provisions in the *Designs Act 2003* (Cth).

82 Additions of legislative provisions enacted since 1991 include: *Aged Care Act 1997* (Cth) ss 86-2(1), 86-5 to 86-7; and *Gene Technology Act 2000* (Cth) s 187(1), (2).

83 Secrecy provisions added to enactments already listed in sch 3 include: *Telecommunications (Interception) Act 1979* (Cth) s 133 and *Taxation Administration Act 1953* (Cth) ss 3G, 3H and sch 1 355–5.

84 See, eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(11); *Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992* (Cth) s 24; *Reserve Bank Act 1959* (Cth) s 79A(9).

85 See, eg, the notes contained in *Gene Technology Act 2000* (Cth) s 197 and *Migration Act 1958* (Cth) s 503A.

86 See, eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(11).

87 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.99].

88 *Kwok v Minister for Immigration and Multicultural Affairs* (2001) 112 FCR 94.

information supplied by law enforcement agencies or intelligence agencies. Notwithstanding that the provision failed the criteria in s 38(1)(b)(ii), Tamberlin J considered that the secrecy exemption applied, because s 503A(8) was ‘cast in comprehensive language’ sufficient to exclude the operation of the FOI Act.<sup>89</sup> The width of the language enlivened the secrecy exemption in the FOI Act, even though that provision was not listed in sch 3 of the FOI Act, nor did it expressly apply the secrecy exemption.

4.64 The decision in *Kwok* has not gone uncriticised, and although the decision was overturned by the Full Federal Court, the secrecy exemption was not considered on appeal. In 2003, s 38 of the FOI Act was amended to make express reference to s 503A, to make clear that a document is exempt to the extent that disclosure is prevented by s 503A of the *Migration Act* and the document contains personal information about a person who has requested access to that document.<sup>90</sup> While this amendment dealt with the immediate problem created by *Kwok* in the interpretation of s 38, it leaves a remaining uncertainty as to whether a secrecy provision may activate the exemption even where the criteria in s 38 are not addressed.

#### ***Comparative secrecy exemption provisions***

4.65 The UK and Canada both include express secrecy exemption provisions in their FOI legislation. New Zealand, in contrast, does not.

4.66 Section 44 of the UK FOI Act provides that information is exempt if its disclosure is ‘prohibited by or under any enactment’. As explained by the Information Commissioner’s Office:

Section 44 is an absolute exemption, which means that if information is covered by any of the subsections in s 44 then it is exempt from disclosure. There is no need to consider whether there might be a stronger public interest in disclosing the information than in not disclosing it. Absolute exemptions contain an inbuilt prejudice test. This test means that the harm to the public interest that would result from the disclosure of information falling within an absolute exemption has already been established.<sup>91</sup>

4.67 Pursuant to this exemption, there are ‘still hundreds of statutory provisions preventing the release of information’, although under s 75 of the UK FOI Act they are subject to review by the Lord Chancellor.<sup>92</sup>

---

89 Ibid, 99. This is the case regardless of whether a relevant Act was enacted before or after the commencement of s 503A of the *Migration Act 1958* (Cth). See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.99].

90 *Migration Legislation Amendment (Protected Information) Act 2003* (Cth) sch 2.

91 Information Commissioner’s Office (UK), *Freedom of Information Act Awareness Guidance No 27: Prohibitions on Disclosure* (December 2004 (updated January 2006)), 1.

92 Information Commissioner’s Office (UK), *Freedom of Information Act Awareness Guidance No 27: Prohibitions on Disclosure* (December 2004 (updated January 2006)), 2.

4.68 The Canadian provision is also in absolute terms. Section 24 of the *Access to Information Act 1985* RSC cA-1 (Canada) provides that:

- (1) The head of a government institution shall refuse to disclose any record requested under this Act that contains information the disclosure of which is restricted by or pursuant to any provision set out in Schedule II.

4.69 This mirrors the current Australian provision by referring to a list of provisions set out in a schedule to the Act. There is, however, an additional subsection, s 24(2), which provides for a committee to be established to review every provision in the schedule and to report ‘on whether and to what extent the provisions are necessary’. The Annual Reports of the Information Commissioner of Canada include a note of whenever sch II is amended.<sup>93</sup>

4.70 In New Zealand, the existence of a secrecy prohibition in another enactment is not of itself a basis of exemption from an application under the *Official Information Act 1982* (NZ). Rather, resisting an application for a document would need to be based on another exception, for example, that the withholding of the information is necessary: to ‘protect the privacy of natural persons, including that of deceased natural persons’;<sup>94</sup> to avoid ‘prejudice to measures protecting the health or safety of members of the public’;<sup>95</sup> or to ‘maintain the effective conduct of public affairs’ through the ‘free and frank expression of opinions by ... officers and employees of any Department or organisation in the course of their duty’.<sup>96</sup>

#### ***Previous inquiries and the secrecy exemption***

4.71 The secrecy exemption in the FOI Act has been considered in a number of previous inquiries. In ALRC 77, the ALRC and ARC recommended that the secrecy exemption should be repealed on the basis that the other FOI exemptions, such as those dealing with personal information and national security and defence, provided sufficient protection of government-held information covered by secrecy provisions.<sup>97</sup> The ALRC and ARC also noted the submission by the Department of Social Security that the 1994 amendments to the *Social Security Act 1991* (Cth), which had removed the secrecy exemption for FOI applications to the Department, had not adversely affected the operations of the Department.<sup>98</sup>

4.72 The ALRC and ARC concluded that:

the exemption provisions in the FOI Act represent the full extent of information that should not be disclosed to members of the public. Secrecy provisions that prohibit the

<sup>93</sup> Office of the Information Commissioner (Canada), *Annual Report* (1999–2000), pt D, II Statutory prohibitions against disclosure of government records.

<sup>94</sup> *Official Information Act 1982* (New Zealand) s 9(2)(a).

<sup>95</sup> Ibid s 9(2)(c).

<sup>96</sup> Ibid s 9(2)(g)(i).

<sup>97</sup> Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 70.

<sup>98</sup> Ibid, [11.3].

disclosure of information that would not fall within the exemption provisions are too broad. The Review considers that repealing s 38 will promote a more pro-disclosure culture in agencies.<sup>99</sup>

4.73 The ALRC and ARC also suggested that, if the secrecy exemption were not repealed, it should be amended so that sch 3 provides a definitive list of all secrecy provisions that affect the operation of the FOI Act.<sup>100</sup>

4.74 In 2001, several recommendations made in ALRC 77 were considered by the Senate Legal and Constitutional Affairs Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (the Senate Committee Inquiry).<sup>101</sup> In its submission to the Senate Committee Inquiry, the Australian Government Attorney-General's Department (AGD) opposed the repeal of s 38 of the FOI Act:

In the Department's view, the exemptions in the FOI Act are, of necessity, in general terms whereas the secrecy provisions in other legislation are tailored to the specific requirements of that legislation and may cover situations, not covered by the FOI Act, which nevertheless warrant exemption from disclosure.<sup>102</sup>

4.75 The Senate Committee Inquiry concluded that the repeal of FOI exemptions, including the secrecy exemption, would be 'premature' and should be considered as part of a 'longer-term revision of the FOI Act'.<sup>103</sup>

4.76 The Solomon Committee gave consideration to the secrecy exemption in the Queensland FOI Act. Rather than retaining a specific exemption for documents subject to a secrecy provision, the Committee recommended that the existence of a secrecy provision be a factor in the assessment of disclosure. This would then be taken into account in the assessment under the proposed single public interest test of general application.<sup>104</sup> Such an approach is consistent with the recommendation in ALRC 77.<sup>105</sup>

---

99 Ibid.

100 Ibid.

101 Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001). This Bill was introduced by Democrats Senator Andrew Murray in 2000, and would have implemented several of the recommendations made by the ALRC and the ARC in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).

102 Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.35].

103 Ibid, [3.34]–[3.36].

104 Freedom of Information Review Panel, *The Right to Information: The Report of the FOI Independent Review Panel* (2008), 156–157, Rec 45.

105 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [11.3].

### An appropriate balance between secrecy and open government?

4.77 One issue in this Inquiry is whether the operation of secrecy provisions contradicts a fundamental premise of the FOI Act. Paterson observes that it is important to scrutinise secrecy provisions ‘to ensure that they do not unnecessarily restrict access’.<sup>106</sup> There is an apparent discrepancy between the objects of the FOI Act—with its presumption of general access to information—and the application of criminal and administrative penalties for informal disclosure in accordance with the intention of the FOI Act.<sup>107</sup> A person who follows the spirit of the FOI Act and discloses a document without having received a formal FOI request may commit a breach of a secrecy provision that would not have been breached if the information had been released pursuant to an FOI application. This has led Christopher Erskine SC to observe that:

the question is no longer the substance of disclosure, but the process by which it happens ... the issue is who makes the decision to release [the records], not whether they are released at all.<sup>108</sup>

4.78 On 31 December 2007, the Department of the Prime Minister and Cabinet released an updated version of the *FOI Guidelines—Exemption Sections in the FOI Act* (the Guidelines). The Guidelines are described as a ‘reference tool’ and do not replace the operation of exemptions in the FOI Act.<sup>109</sup> The Guidelines note that the secrecy exemption ‘should be used only where truly necessary’ and that information may be more appropriately considered under other exemptions in the FOI Act. The Guidelines also state that the exemption is not intended to include information that is ‘identified by reference only to the manner or capacity in which it is received’.<sup>110</sup>

4.79 The FOI Exposure Draft Bill also includes new protection provisions against criminal liability where, for example, access to a document is given in good faith either in response to a request, or in the belief that access is permitted.<sup>111</sup>

---

106 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.105].

107 A person who makes an informal disclosure in accordance with the object of the FOI Act does not receive the same protection as a person who makes a formal disclosure under the Act. Paterson has described the ‘chilling effect’ of secrecy provisions in this context: *Ibid*, [8.106]. See also the discussion of public interest disclosure (or ‘whistleblowing’) legislation in Chs 9 and 11.

108 C Erskine, ‘The Bennett Decision Explained: The Sky is not Falling!’ (2005) 46 *Australian Institute of Administrative Law (AIAL) Forum* 15, 18.

109 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2007) <[www.dpmc.gov.au](http://www.dpmc.gov.au)> at 14 October 2008. Agency policies for information handling, which may include FOI matters, are discussed in Ch 15.

110 *Ibid*, [9.1.4]. See also Australian Government Attorney-General’s Department, *Freedom of Information Act 1982—Fundamental Principles and Procedures* (2005) <<http://www.pmc.gov.au>> at 21 November 2008.

111 Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, cl 92.

## **Submissions**

4.80 In IP 34, the ALRC asked specific questions as to the secrecy exemption, focusing both on the interrelationship between the FOI Act and secrecy provisions generally, as well as the specific operation of the secrecy exemption.<sup>112</sup> The ALRC also revisited the recommendation made in ALRC 77, that the secrecy exemption in s 38 should be repealed.

4.81 A number of themes were evident in submissions: the role of public interest in the FOI Act; the tension between FOI and secrecy; uncertainty and practical difficulties in the operation of the secrecy exemption; support for retention of s 38; and support for repeal of s 38.

### ***Public interest in the FOI Act***

4.82 Several stakeholders used the opportunity to remark broadly on the role of public interest in the FOI Act, for example:

Liberty Victoria understands that the release and retention of government information represents a balancing of interests, and the circumstances in which we, as the public, accede to a shift in that balance in the name of our interest. As noted on Page 19 of [IP 34], the real public interest lies in an open and accountable government. It is for this reason that Liberty Victoria takes the opportunity to make the important distinction between the ‘public interest’ in information release and a competing ‘national interest’ in its retention. In particular, Liberty Victoria advocates a narrow definition of national interest which would restrict the retention of government documents, and a broader definition of public interest facilitating their release in prescribed circumstances.

For instance, information withheld in the national interest may be limited to particular interests such as national security and cabinet-in-confidence. Other ‘national interests’ such as commercial sensitivity or impartiality of the public service will be more circumstantial while others should be excluded entirely.<sup>113</sup>

4.83 Similarly, Australia’s Right To Know (ARTK) coalition stated that access to information should be provided ‘as of right’. The only exception would be where, on balance, such access ‘is demonstrably contrary to the protection of essential public interests’, to be tested against a single public interest test that states:

Access is to be provided to government information unless its disclosure is demonstrably contrary to the public interest.<sup>114</sup>

4.84 The result, the ARTK coalition argued, would be that:

Measures such as these will contribute to a socio-political culture which embraces openness and transparency, holding at its core the assumption that government

<sup>112</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Questions 7–1 to 7–3.

<sup>113</sup> Liberty Victoria, *Submission SR 19*, 18 February 2009.

<sup>114</sup> Australia’s Right to Know, *Submission SR 35*, 6 March 2009.

information is ultimately owned by all citizens, held on trust by their government for their benefit, and to be made available to further their rights and purposes and those of the national interest.<sup>115</sup>

### **Tension between FOI and secrecy**

4.85 That there is tension between the regimes was identified by the Public Interest Advocacy Centre (PIAC):

There is a clear tension when information that would otherwise be subject to secrecy or non-disclosure provisions also falls within the access regime established by the FOI Act, and is otherwise available for release. For example, the very broad prohibition set out in section 70 of the Crimes Act relating to communication of government information, regardless of its nature or significance, appears diametrically opposed to the policy objectives sought to be achieved by the FOI Act.<sup>116</sup>

4.86 The interconnectedness of secrecy and FOI was also clearly identified in the submission from the Australian Press Council:

When considering the level of government openness, secrecy laws cannot be assessed separately to Freedom of Information legislation. Many of the issues that arise in relation to secrecy legislation also arise in relation to Freedom of Information law. It is a curious paradox that legislation, which was introduced for the purpose of increasing public access to government information, is often relied upon by governments in blocking such access. Reform of secrecy laws will achieve very little if Freedom of Information is not reformed at the same time. As with secrecy law reform, Freedom of Information legislation should be formulated so that open access is the default, with access only being denied where disclosure would be likely to cause damage to the public interest.<sup>117</sup>

4.87 The Community and Public Sector Union (CPSU) also expressed concerns about the operation of the secrecy exemption in the context of a commitment to open government:

The notion of open and transparent government should be the guiding principle in approaching issues of the ability of the public to obtain information about their Government. The CPSU is concerned that any changes to secrecy provisions to clarify their scope or application must be tailored to fit with the principles of open and transparent government and legislation dealing with freedom of information and privacy. Secrecy provisions and public access to information should not be viewed as opposed to one another, but complementary.<sup>118</sup>

4.88 The Department of Human Services (DHS) argued for a closer connection between the underlying structure of the FOI Act and secrecy provisions:

From a theoretical standpoint, there would seem to be no justification for the protection under secrecy laws of information which would be released under the FOI

---

115 Ibid.

116 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

117 Australian Press Council, *Submission SR 16*, 18 February 2009.

118 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

Act. The question then becomes whether the basis for exempting information from disclosure under the FOI Act (which reflects the Government's policy in this regard) should also provide the basis for the scope of protection afforded by secrecy provisions.<sup>119</sup>

4.89 It was also submitted by PIAC that:

It could be argued that the relationship between the FOI Act and secrecy provisions in other Acts would be better balanced were the existence of a secrecy provision in another Act sufficient to give rise only to a *prima facie* claim for FOI exemption, with the claim itself to be tested by reference to the range of exemptions and machinery provisions which the FOI Act itself sets out.<sup>120</sup>

4.90 It also supported the repeal of the current secrecy exemption, which is considered below.

### ***Uncertainty and practical difficulties***

4.91 Uncertainty in the present working of the secrecy exemption was a recurring theme. The AGD was concerned as to a lack of clarity in several respects:

Many secrecy laws provide an exception for disclosure ‘in accordance with the law’ or ‘as authorised by law’, which would seem to permit a document containing that information being disclosed pursuant to the FOI Act if no exemptions apply. Secrecy laws listed in schedule 3 of the FOI Act or that expressly enliven section 38 of that Act provide clear guidance that documents to which secrecy laws apply are exempt documents under the FOI Act. Uncertainty may arise if the secrecy law neither enlivens section 38 nor contains an exception permitting disclosure in accordance with or authorised by law. In these cases a potential conflict of laws situation arises, and the interaction between the secrecy law and the FOI Act may depend on the interpretation of the specific provision. ...

It might be helpful to clarify that a disclosure of a document authorised under the FOI Act does not constitute an offence under secrecy laws. As discussed above, this is likely to simply clarify the position, since most secrecy laws would expressly or impliedly permit disclosures that are authorised by law. Where there are strong grounds for a secrecy law to operate to prevent release of documents under the FOI Act, this should be made clear to avoid any uncertainty. Retaining section 38 of the FOI Act and listing relevant provisions in schedule 3 might be one way to ensure the interaction between such secrecy provisions and the FOI Act are clear, noting that agencies would need to justify the inclusion of their secrecy provision in schedule 3.<sup>121</sup>

---

119 Department of Human Services, *Submission SR 26*, 20 February 2009.

120 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

121 Attorney-General’s Department, *Submission SR 36*, 6 March 2009. The Australian Securities and Investments Commission also pointed to the need for clarification within s 38 ‘to make the circumstances of its application more clear’, Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

4.92 The Australian Taxation Office (ATO) identified ‘practical difficulties’ in the current operation of the two limbs of s 38:

if a tax secrecy provision is not listed in Schedule 3 to the FOI Act, or does not otherwise apply section 38 ... to the relevant information, the ATO may not be able to resist the disclosure of information under the FOI Act which would otherwise constitute a criminal offence.<sup>122</sup>

4.93 To address such problems the ATO suggested that

there may be preferable models of ensuring that the FOI Act does not impede the confidentiality of taxpayer information. For example, the FOI Act could exempt documents (and the information contained therein) from release where a tax secrecy provision applied to protect the documents or information. This approach would be similar to the approach taken in the *Archives Act 1983* (Archives Act), which exempts information from being released under that Act where ‘there is in force a law relating to taxation that applies specifically to information or matter of that kind and prohibits persons referred to in that law from disclosing information or matter of that kind, whether the prohibition is absolute or is subject to exceptions or qualifications’ (see paragraph 33(3)(b) of the Archives Act).<sup>123</sup>

4.94 In its submission, which was in favour of repeal, PIAC also identified the ‘lack of coherence in the range and seriousness of matters excluded from FOI law by the operation of section 38’.<sup>124</sup>

4.95 The Commonwealth Ombudsman noted the impediment s 38 posed to investigating complaints referred to the Ombudsman:

Another situation where Ombudsman investigations encounter difficulty with secrecy provisions is where a complaint is received from a person that their FOI request was denied because of the operation of a secrecy provision. An enthusiastic reliance by the agency on its own secrecy provision can impede efficient investigation of that complaint by the Ombudsman in a context where the use of the provision was not intended.<sup>125</sup>

4.96 Other stakeholders remarked on specific aspects or difficulties experienced with the FOI Act more generally. For example, The Fairness in Child Support Group took issue with the wording of Question 7–1 in IP 34 and the reference to the FOI Act as promoting open and accountable government. The Group recommended ‘the removal of exemptions to the FOI Act that apply to the Child Support Agency and the Family Court of Australia’.<sup>126</sup>

---

122 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

123 Ibid. The interrelation between secrecy provisions and the *Archives Act 1983* (Cth) is considered below.

124 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009. This submission is also referred to below, in relation to repeal of *Freedom of Information Act 1982* (Cth) s 38.

125 Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009.

126 Fairness in Child Support, *Submission SR 23*, 19 February 2009.

### ***Retaining secrecy exemptions***

4.97 The Australian Intelligence Community (AIC) argued strongly in favour of retaining the exempt status of AIC agencies—also recommended in ALRC 77<sup>127</sup>—and that the FOI Act ‘should recognise and not override national security secrecy provisions in any circumstances’.<sup>128</sup>

4.98 The ATO and the Australian Prudential Regulation Authority (APRA) also supported the retention of the secrecy exemption in s 38. The ATO was concerned that a repeal of the exemption

could potentially result in anomalous levels of protection for taxpayer information and create uncertainty for both taxpayers and tax officers who are responsible for making decisions under the FOI Act.<sup>129</sup>

4.99 The Treasury echoed such concerns:

If section 38 were to be repealed, then in order to give effect to legitimate expectations of taxpayers to ensure the protection of their information, such information would need to come within one of the other exceptions listed in the FOI Act. While there appears to be broad consistency in the type of information that can be disclosed under secrecy and FOI law, the ATO’s submission on this issue highlights one instance where the FOI exemptions may, but for section 38, be insufficient in resisting the release of information that is otherwise protected under taxation secrecy provisions.

When such inconsistencies do arise, the issue then appears to become whether the secrecy provisions (by virtue of section 38) or the FOI Act provisions take precedence. While it is important to ensure that secrecy provisions, such as those in the taxation law, are developed in a manner that is consistent with the objects of the FOI Act and do not seek to undermine the goal of open and transparent Government, we consider that the secrecy provisions are best placed to address the unique characteristics of taxpayer information and the context in which they are provided.<sup>130</sup>

4.100 In its submission, APRA also supported the retention of the secrecy exemption in s 38 of the *Australian Prudential Regulation Authority Act 1998* (Cth).

APRA is strongly of the view that s 38 should remain in the FOI Act and that s 56 should continue to specify that it attracts the exemption in s 38. In the absence of s 38 there would be scope for protected documents to be obtained under FOI, substantially weakening the effectiveness of the secrecy provision, with adverse consequences for APRA’s relationship with regulated entities and foreign regulators (and therefore the overall effectiveness of APRA’s prudential regulation). In particular, APRA does not consider that s 43 of the FOI Act (business information) would be a practical alternative in all circumstances as there could be differences of opinion as to whether the conditions in that section are satisfied in relation to individual items of

127 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.

128 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

129 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

130 The Treasury, *Submission SR 22*, 19 February 2009.

information. In addition, if s 38 were repealed, APRA would likely become subject to a greater number of FOI applications from third parties seeking information about regulated entities, such as parties to unrelated civil litigation. This would have the practical effect of forcing APRA to redirect resources away from its supervisory functions and into the FOI function.<sup>131</sup>

### ***Repealing the secrecy exemption***

4.101 A number of stakeholders supported the repeal of s 38 recommended in ALRC 77, on the basis that the other exemption categories were sufficient to provide protection even where secrecy provisions existed. For example, the ARTK coalition submitted that:

it is difficult to conceive of circumstances where information protected by secrecy provisions would not also fall within other exemptions in the Act, such as documents containing information the disclosure of which would prejudice national security, defence or international relations, or constitute a breach of Cabinet confidence, and so forth. This approach would then be consistent with the similar exemption regime for access to documents under the *Archives Act 1983* (Cth).<sup>132</sup>

4.102 One caller to the secrecy phone-in objected to ‘blanket exemptions’ in general, because, the caller stated, they ‘make people lazy’.<sup>133</sup>

4.103 Some stakeholders submitted that if a secrecy exemption like s 38 were retained, it should be subject to a public interest test. For example, the Media, Entertainment & Arts Alliance advocated that:

the preferred approach is that taken by the NSW Freedom of Information Act 1989 which, rather than applying a blanket exemption to all such documents irrespective of their content, instead provides an exemption for documents dealing with law enforcement, public safety or anti-terrorism measures, except for documents, or information, which reveal that the scope of law enforcement investigation has exceeded the limit imposed by law and whose disclosure would be in the public interest.<sup>134</sup>

4.104 As PIAC suggested, in some contexts there may be a *prima facie* exemption, but the object of openness should be paramount:

It might be thought, for example, that the fact that a document was prepared by or received from a security agency could give rise to a *prima facie* exemption. In PIAC’s view, the exemption itself should be tested having regard to the content of the document itself, the possible consequences of release, and any positive public interest factors in favour of disclosure.

---

131 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

132 Australia’s Right to Know, *Submission SR 35*, 6 March 2009.

133 *Secrecy Phone-In*, 11–12 February 2009.

134 Media Entertainment & Arts Alliance, *Submission SR 39*, 10 March 2009. The particular exemption category behind these comments is sch 1, cl 4 of the *Freedom of Information Act 1989* (NSW), which applies to documents affecting law enforcement and public safety.

The current review provides a valuable opportunity to consider whether the introduction of a further layer of procedural safeguards to the existing provisions under the FOI Act should lend weight to the policy option set out in question 7-2 of the Issues Paper. In PIAC's view, disclosure in accordance with the objects of and subject to the exemptions set out in the FOI Act should override secrecy provisions in other Acts.<sup>135</sup>

4.105 In a very lengthy and informative submission, Ron Fraser commented that while simply repealing s 38 might not be as straightforward as proposed in ALRC 77 with respect to whether the other exemption provisions would provide the full scope of protection,

... at the very least a very large number of secrecy provisions currently subject to s 38 do not warrant that protection.

The other exemption provisions of the FOI Act are well designed to protect much of the information protected by secrecy provisions. ... [And] consideration of access rights under [other] exemptions, where applicable, is strongly preferable to absolute protection of the same information under secrecy provisions protected by s 38.<sup>136</sup>

4.106 Fraser objected to the width of secrecy provisions such that 'innocuous information as well as genuinely sensitive information' may be caught. He suggested—consistent with the submission of the AGD to the Senate Legal and Constitutional Committee in 2001 when opposing repeal of s 38<sup>137</sup>—that other exemptions of the FOI Act 'should be permitted to do their work'. Hence, he argued, the only secrecy provisions that should be included in the ambit of an exemption provision like s 38, are 'those that protect information, access to which cannot be determined under other FOI exemptions', so long as such a provision 'not be used as an unwarranted means to expand widely the categories of information not open to access under the FOI Act'. A secrecy exemption should, therefore, be confined 'to its proper role as a complementary provision to the largely harm-based scheme of the FOI Act'.<sup>138</sup>

4.107 Following such an approach, Fraser proposed that the criteria for retaining any secrecy provisions as exemptions to the FOI Act should be on the basis that:

there are no exemptions in the FOI Act which would apply to the information with which they are concerned, and that disclosure could be expected to cause substantial damage to a public interest.<sup>139</sup>

---

135 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

136 R Fraser, *Submission SR 42*, 23 March 2009.

137 Referred to in Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), [7.27].

138 R Fraser, *Submission SR 42*, 23 March 2009. So, for example, he suggested that the exemptions concerning personal information and business affairs, which already include a number of safeguards or thresholds before disclosure, are 'well-adapted to consideration of the kinds of information covered by secrecy provisions that apply to "information relating to the affairs of a person"'.

139 Ibid.

4.108 The inclusion of a public interest test, he argued ‘goes to the heart of modern access law as against provisions based on the model of highly controlled secrecy with discretionary disclosures’.<sup>140</sup> As to the kind of public interest that might be included, Fraser submitted that ‘a standard balancing public interest test or an override public interest power at the external review stage’ was the preferable model.<sup>141</sup>

### ALRC’s views

4.109 A central focus of this Inquiry is to identify the harms caused by disclosure of Commonwealth information that justify the imposition of criminal sanctions or administrative penalties. In later proposals in this Discussion Paper, the ALRC seeks to strike the appropriate balance between protecting essential public interests while ensuring an appropriate level of openness and transparency in government.

4.110 In ALRC 77, the repeal of s 38 was recommended.<sup>142</sup> Although the ALRC and ARC noted that many agencies were concerned that were s 38 to be removed, information covered by the secrecy provisions would not be exempt under any other provision of the FOI Act, the ALRC and ARC were ‘not convinced’ by that argument:

Taxpayer information is provided pursuant to statutory obligations, not voluntarily. In addition, taxpayer information is adequately protected under the exemptions for personal and business information. In most, if not all, cases the FOI exemptions cover government-held information currently protected by a secrecy provision. ...

[T]he Review considers that the exemption provisions in the FOI Act represent the full extent of information that should not be disclosed to members of the public. Secrecy provisions that prohibit the disclosure of information that would not fall within the exemption provisions are too broad. The Review considers that repealing s 38 will promote a more pro-disclosure culture in agencies. ... If s 38 is not repealed, it should at least be amended so that Schedule 3 becomes a definitive list of all secrecy provisions to which the FOI Act is subject.<sup>143</sup>

4.111 As the submissions above demonstrate, there is still concern expressed by some agencies that the removal of s 38 would compromise the strength of secrecy provisions, thereby undermining the confidence of those individuals and businesses or organisations providing information to agencies. Agencies continue to express concern that the other exemption provisions in the FOI Act will not provide sufficient protection, or may prejudice the future supply of information to agencies.

4.112 If, by way of example, disclosure of taxation information about an individual would have a substantial adverse effect on their willingness to provide information to the ATO, thereby jeopardising the future supply of such information, then it would seem such disclosure would be ‘unreasonable’ under s 41 of the FOI Act. However, as

---

140 Ibid.

141 Ibid.

142 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 70.

143 Ibid, 146 (notes omitted).

noted in ALRC 77, much taxation information is provided pursuant to an obligation and not voluntarily. In the case of a business, if the disclosure of information could reasonably be expected to prejudice the future supply of information to the ATO, then the information would appear to be exempt under s 43. Additionally, s 45 would operate to exempt information the disclosure of which would found an action for breach of confidence. This should remain so, even where a public interest test applies to the exemption provisions.

4.113 However, as Paterson has observed, the approach in the current form of s 38 has considerable merit both in terms of simplicity and in ensuring a more considered approach to the question of which secrecy laws should take precedence over the access provisions in the FOI Act.<sup>144</sup>

4.114 Paterson directs attention rather at the ‘chilling effect’ of the large number of secrecy laws:

including the category of general secrecy provisions which prohibit the disclosure of information acquired by government officers in the course of their duties. General secrecy provisions have a very wide operation and effectively prohibit the revelation, whether deliberate or accidental, oral or in writing, of any thing that is secret. Liability does not depend on the nature or sensitivity of the information in question and reflects an outdated view that the general public has no legitimate concern about the processes of government.<sup>145</sup>

4.115 As evident in other chapters in this Discussion Paper, a major concern expressed in submissions and consultations—and consonant with the observations of Paterson—is with respect to the width of current secrecy provisions and the inconsistent, and often severe, penalty regimes that potentially apply. A large number of the ALRC’s proposals are therefore focused on achieving a principled basis for secrecy provisions across the range.

4.116 At the same time, the ALRC has developed a range of proposals in this Discussion Paper focused upon the whole spectrum of the handling of Commonwealth information, from improving the awareness and understanding of secrecy obligations, to the nature of liability and penalties that should be imposed in the event of breach. These, together with a shift towards a pro-disclosure culture, by improved and clearer agency practices, are aimed at achieving consistency, clarity and a better balance of the public interests in play.

4.117 The ALRC is of the view that the proposal made in ALRC 77 is consistent with this approach. It is also consistent with the pro-disclosure model reflected in the FOI Exposure Draft Bill, notwithstanding the absence of any mention of s 38.

---

<sup>144</sup> M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.105].

<sup>145</sup> Ibid, [8.106].

4.118 As discussed in Chapter 6, the idea of essential public interests as reflected in the FOI Act forms the backbone of the proposed new general secrecy offence. The ALRC takes the view that the exemption provisions—apart from s 38—do provide sufficient protection of these essential public interests, and that consideration of documents on a case-by-case basis is a more effective method for ensuring that only truly sensitive information is placed outside the reach of the ordinary citizen.

4.119 The FOI Act includes mechanisms for the protection of certain documents and agencies where such documents and agencies are considered as needing heightened protection by means of express exempt status. The repeal of s 38 would not affect the ability of the Australian Parliament to make such designation in appropriate circumstances, such as national security. In announcing the release of the FOI Exposure Draft Bill, Senator Faulkner reiterated the importance of the current exempt status of national security agencies and documents, for example.<sup>146</sup>

4.120 If s 38 were repealed, then the existence of a secrecy provision would form an important factor to be weighed when considering disclosure under another exemption provision. In the language of the conditional exemptions in the FOI Exposure Draft Bill, they would be subjected to a consideration of whether disclosure would be ‘contrary to the public interest’, using the factors spelled out in the Bill.

4.121 The ALRC proposes that if s 38 is repealed then the FOI Guidelines should be updated to provide guidance to FOI officers, especially with reference to the existence of a secrecy provision being an appropriate consideration when evaluating whether information should be disclosed under other exemption provisions.

4.122 In this context, the ALRC considers that the current FOI Guidelines or the proposed Information Commissioner Guidelines referred to in cl 93A of the FOI Exposure Draft Bill, are an appropriate tool to ensure that officers are aware of and understand their obligations in this regard. The Guidelines should be amended to make particular reference to the existence of a secrecy provision as being a factor in weighing up whether an exemption should be made from disclosure in a particular case. This is also consistent with the recommendations made by the Solomon Committee.

4.123 Alternatively, if s 38 were retained, then clarity in its operation is essential. In this regard any new secrecy provision should clearly address the intersection of the provision with the FOI Act. It should also be included in sch 3. Further, sch 3 needs to be reviewed against the pro-disclosure objects of the FOI Exposure Draft Bill and regularly updated. If the proposed FOI Commissioner is introduced, the responsibility for ensuring that sch 3 accurately lists secrecy provisions that trigger the secrecy exemption would rest appropriately with that office.

---

146 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

4.124 To prompt further consideration of the intersection between the FOI Act and secrecy provisions the ALRC proposes the repeal of s 38.

**Proposal 4–1** Reflecting a commitment to open government and to ensure that claims for exemption be considered on a case by case basis rather than through the mechanism of a global exemption for secrecy provisions, s 38 of the *Freedom of Information Act 1982* (Cth) should be repealed.

**Proposal 4–2** The Office of Parliamentary Counsel should issue a Drafting Direction that any proposed secrecy provision must indicate expressly whether it overrides the *Freedom of Information Act 1982* (Cth).

**Proposal 4–3** If s 38 of the *Freedom of Information Act 1982* (Cth) is repealed, the *FOI Guidelines—Exemption Sections in the FOI Act* issued by the Department of the Prime Minister and Cabinet or the proposed Information Commissioner Guidelines should be updated to inform Freedom of Information officers that the existence of a secrecy provision is a relevant factor to consider when deciding whether or not to disclose a document.

**Proposal 4–4** If s 38 of the *Freedom of Information Act 1982* (Cth) is retained, the responsible minister (or the proposed Freedom of Information Commissioner) should ensure that the list of secrecy provisions in sch 3 of the Act is regularly reviewed and updated.

## Archives

### Overview of the *Archives Act 1983* (Cth)

4.125 The FOI Act and the *Archives Act* were both introduced as part of a package of administrative law reforms in the early 1980s. Both Acts deal with access to documents and records, and are interconnected, the *Archives Act* being drafted ‘to dovetail’ with the FOI Act.<sup>147</sup>

4.126 The *Archives Act* established the National Archives of Australia (NAA) and set out comprehensive arrangements for conserving and preserving the archival resources of the Commonwealth.<sup>148</sup> As noted in ALRC 77, the role of the NAA includes:

encouraging and facilitating the use of archives, developing policy and advice for government agencies on the management, preservation and disposal of records and

---

147 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [5.59].

148 *Archives Act 1983* (Cth) pt V.

creating and maintaining information systems about the structure of government and the Commonwealth's record series.<sup>149</sup>

4.127 The NAA is responsible for providing public access to government records that are more than 30 years old. Similar to the FOI Act, however, there are exemptions to such access. Further, some categories of record may not be disclosed for periods longer than 30 years. For Cabinet notebooks the period is currently 50 years; and for census information the period is 99 years.<sup>150</sup> Under proposed amendments in the FOI Exposure Draft Bill the open access periods for most records will be reduced to 20 years and Cabinet records to 30 years.<sup>151</sup>

## Exemptions

4.128 The *Archives Act* does contain some exemptions for access to records in the open access period, but these exemptions are less restrictive than those under the FOI Act because the records sought are older and generally less sensitive. Section 33 of the *Archives Act* provides that a Commonwealth record is an exempt record if it contains information or matter of particular kinds, including, for example, information that:

- could reasonably be expected to cause damage to the security, defence or international relations of the Commonwealth;
- is communicated in confidence by or on behalf of a foreign government;
- if disclosed, would, or could reasonably be expected to prejudice the investigation of a breach of the law, prejudice the fair trial or endanger the life or physical safety of any person;
- would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person).<sup>152</sup>

4.129 There is a clear relationship between the exemption provisions in the *Archives Act* and the FOI Act. As noted by Paterson:

[the] exemption provisions, although differently worded, cover similar ground to a number of the exemption provisions in the Commonwealth FOI Act and they share many [of the same] drafting characteristics. They make reference to many similar concepts such as 'substantial adverse effect' and reasonableness. Given that the *Archives Act* was specifically drafted to dovetail with the Commonwealth FOI Act,

---

<sup>149</sup> Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [5.3].

<sup>150</sup> *Archives Act 1983* (Cth) ss 22A, 22B.

<sup>151</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 1; J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009), 10.

<sup>152</sup> *Archives Act 1983* (Cth) s 33(1)(a), (b), (e)(i), (f)(i) and (iii), (g).

those expressions arguably convey similar meanings to those discussed ... in relation to freedom of information laws.<sup>153</sup>

4.130 Information collected for taxation purposes is also singled out as requiring a particular exemption, in s 33(3):

- (3) For the purposes of this Act, a Commonwealth record is an exempt record if:
  - (a) it contains information or matter:
    - (i) that relates to the personal affairs, or the business or professional affairs, of any person (including a deceased person); or
    - (ii) that relates to the business, commercial or financial affairs of an organization or undertaking; and
  - (b) there is in force a law relating to taxation that applies specifically to information or matter of that kind and prohibits persons referred to in that law from disclosing information or matter of that kind, whether the prohibition is absolute or is subject to exceptions or qualifications.

4.131 In the 1998 Report, *Australia's Federal Record: A Review of Archives Act 1983* (ALRC 85), the ALRC considered the exemptions in the *Archives Act* and recommended that the number of categories for exempt documents be reduced. In particular, the ALRC recommended that s 33(3) be repealed.<sup>154</sup>

4.132 The ALRC also recommended that the Act be amended to include an exemption category relating to information that, under Indigenous tradition, is confidential or subject to particular disclosure restrictions.<sup>155</sup>

4.133 On 1 November 2008, the *Archives Amendment Act 2008* (Cth) came into operation. This Act implements several of the recommendations made in ALRC 85, but the Act does not remove any exemptions from the *Archives Act*.<sup>156</sup>

### **Secrecy and the *Archives Act***

4.134 Whereas the FOI Act has an express exemption which refers to secrecy provisions—in s 38—the *Archives Act* does not. It does, however, give particular attention to census information and refer to taxation secrecy provisions, as noted above.

---

153 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [5.59].

154 Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Rec 167.

155 Ibid, Rec 164. The ALRC recommended that the language of this category should be consistent with that of the exemption proposed in the Aboriginal and Torres Strait Islander Heritage Protection Bill 1998. The ALRC also recommended that a similar exemption be included in the FOI Act: Rec 165.

156 The *Archives Amendment Act 2008* (Cth) inserts an objects clause into the *Archives Act 1983* (Cth) and makes changes to ensure that records remain in the ‘care’ of the NAA when in custody of persons other than the NAA.

4.135 Census information, for example, is given specific protection. The *Archives Act* was amended by the *Census Information Legislation Amendment Act 2000* (Cth) to provide the 99 year period of protection and also to subject Archives officers to a particular duty of non-disclosure set out in s 30A:

- (1) An Archives officer must not, at any time before a record containing Census information from a Census is in the open access period for that Census, divulge or communicate any of that information to another person (except to another Archives officer for the purposes of, or in connection with, the performance of that other officer's duties under this Act).

4.136 The effect of s 30A is to create a secrecy provision within the *Archives Act* itself, applicable to Archives officers and extending to the whole period of protection for census records. The duty extends both to non-disclosure to another person and in proceedings before a court or tribunal.<sup>157</sup> The duty is expressed to give rise to criminal liability through the operation of s 70 of the *Crimes Act 1914* (Cth). The interaction between duties such as s 30A and the general secrecy offence is considered in Chapter 6.

4.137 In addition, Archives officers, as persons engaged under the *Public Service Act 1999* (Cth), are also subject to non-disclosure provisions that apply to them in that capacity, including under the *Public Service Regulations 1999* (Cth). Secrecy obligations under the *Public Service Regulations* are considered in Chapter 13.

4.138 The object of the specific amendments made by the *Census Information Legislation Amendment Act* were:

to ensure that name-identified 2001 Census information, relating only to those households which provide explicit consent, will be stored by the National Archives of Australia to be preserved for release for future genealogical and other research after a closed access period of 99 years. ...

Subsection 30A(1) removes any doubt that Archives officers may not release the Census information in the closed access period ... Subsection 30A(2) protects the 2001 Census information in the custody of Archives from disclosure under compulsion of a court or tribunal and prevents information being provided voluntarily by Archives in evidence before a court or tribunal. Subsection 30A(3) ensures that this provision prevails over Section 58 which would otherwise allow Archives to disclose the Census information where it was proper to do so or required by law.<sup>158</sup>

4.139 While the *Archives Act* does not contain a specific secrecy exemption, information or documents that are subject to non-disclosure provisions may fall within a number of exemptions set out in the Act. The only express secrecy exception is in relation to taxation secrecy, as set out above.

---

157 *Archives Act 1983* (Cth) s 30A(2).

158 Explanatory Memorandum, *Census Information Legislation Amendment Bill 2000* (Cth).

4.140 The ALRC recommendations in ALRC 85 included:

- the repeal of s 33(2) which exempts records covered by client professional privilege;<sup>159</sup>
- the repeal of s 33(3);<sup>160</sup> and
- the amendment of the *Archives Act* to provide expressly that non-disclosure provisions in other legislation do not override the public access provisions of the archives legislation unless this is expressly provided for in the legislation concerned.<sup>161</sup>

4.141 In addition to proposed amendments to the FOI Act, the FOI Exposure Draft Bill also proposes amendments to the *Archives Act* by bringing forward the open access period for most records, as noted above. As explained in the *Companion Guide*:

The effect of this measure is that Cabinet records (other than Cabinet notebooks) and other Government records will be disclosed after 20 years, and Cabinet notebooks will be disclosed after 30 years. All material disclosed under the *Archives Act* will be subject to withholding information which continues to be sensitive in line with exemptions under that Act.<sup>162</sup>

4.142 The proposed amendments leave untouched the closed period for census records of 99 years from the date of a census, under s 22B.

4.143 In IP 34, the ALRC sought comments on how the relationship between secrecy provisions and the *Archives Act* is working in practice, and, if there are any concerns, how these should be addressed.

## **Submissions**

4.144 Only a few stakeholders commented with respect to secrecy provisions and the *Archives Act*.<sup>163</sup> The Australian Bureau of Statistics (ABS) and the ATO strongly defended the retention of specific exemptions with respect to their areas of operation.

4.145 Liberty Victoria supported records becoming available to the public after the specified period, because '[s]uch laws promote open and accountable government' and agreed that that the number of exemption categories under the *Archives Act* should be

---

159 Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Rec 166.

160 Ibid, Rec 167.

161 *Archives Act 1983* (Cth), Rec 108.

162 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009), 10.

163 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; National Archives of Australia, *Submission SR 29*, 23 February 2009; Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009.

reduced, as recommended in ALRC 85.<sup>164</sup> It also argued for a more open approach to information generally:

Liberty Victoria believes that non-secret information should be available to the public on demand at any time. Rather than exempt secret information from archives laws, information should be reviewed and reclassified periodically. Top level information (i.e. NSI—top secret) may cease to be classified at all 50 years later while low level information (i.e. personal information) will remain classified as such for the lifetime of the person. Where strongly in the public interest to do so, classified information may be released.

This approach largely accords with existing exemptions since and provides a more uniform approach, particularly when transitioning information from current to archival.<sup>165</sup>

4.146 The ABS strongly emphasised the importance of confidentiality with respect to the information obtained in censuses, and the need to back this up with secrecy provisions. With respect to the *Archives Act*, the ABS considered that the amendments made in 2000, referred to above, achieved the protection of census data through the introduction of the closed period of 99 years. In view of that, ‘[t]he ABS does not believe that the relationship between the secrecy provisions in the *Census and Statistics Act 1905* and the *Archives Act 1983* needs to be clarified’.<sup>166</sup>

4.147 The ATO also stressed the importance of the maintenance of strict confidentiality in relation to taxation information and argued for the retention of the taxation secrecy exemption in s 33(3), notwithstanding that ALRC 85 had recommended its repeal.<sup>167</sup>

Parliament has specifically exempted taxpayer information from being released under the *Archives Act* after a 30 year period where a tax secrecy provision applies to protect that information. Tax secrecy provisions continue to apply to protect the confidentiality of taxpayer information indefinitely, which the ATO considers is extremely important to maintain the integrity of the tax system and taxpayer confidence in it.<sup>168</sup>

4.148 In contrast, NAA agreed with the recommendation in ALRC 85 that s 33(3) of the *Archives Act* should be removed and argued that ‘secrecy provisions in other legislation should not specifically extend protection to open access period records’:

Exemption categories in the *Archives Act* contain robust protection against the release of any information that remains sensitive beyond 30 years. Section 33 exemption categories allow the National Archives to withhold information from public release on

<sup>164</sup> Liberty Victoria, *Submission SR 19*, 18 February 2009; Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998).

<sup>165</sup> Liberty Victoria, *Submission SR 19*, 18 February 2009.

<sup>166</sup> Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

<sup>167</sup> In a submission to the ALRC in the *Archives Act* inquiry, the ATO had similarly pressed the case for retention: Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), [20.76]–[20.79].

<sup>168</sup> Australian Taxation Office, *Submission SR 13*, 16 February 2009.

[specific grounds]. At 30 years, information should be assessed against these exemption categories to determine an ongoing need for protection rather than having the blanket coverage of secrecy provisions which may result in information being withheld indefinitely and permanently from public scrutiny.

The National Archives argues instead that the *Archives Act* should clearly state that it overrides secrecy provisions for records in the open access period subject to any exemption covered by Section 33, as it does for classified records at Section 59. ...

Whilst the relationship between secrecy provisions and the *Archives Act* generally works well, in part because many of the records covered by such provisions are lawfully disposed of before they reach 30 years, the lack of any clear statement in the Act has meant that in infrequent, but significant cases, it has caused problems.<sup>169</sup>

4.149 The NAA referred to having to seek legal advice on five occasions between 1985 and 1998 confirming its view ‘that the *Archives Act* has primacy over confidentiality or secrecy provisions in a number of other Acts’.<sup>170</sup> In these circumstances, the NAA considered that clarification of the relationship between secrecy provisions and the *Archives Act* could be achieved

by insertion of a clause in the latter Act confirming such provisions cease to apply to records properly made available for public access (ie records assessed against the exemption categories set out in Section 33). Such a clause would resolve current uncertainty, while at the same time providing necessary ongoing protection for sensitive information.<sup>171</sup>

### **ALRC’s views**

4.150 There are two main issues that emerged in submissions: the repeal or retention of s 33(3) and the introduction of a clarifying provision in terms suggested by the NAA. It is clear, however, that any amendment of the FOI Act needs to take into account the impact on the *Archives Act*.

#### ***Repeal of s 33(3)?***

4.151 In ALRC 85, the competing arguments in relation to s 33(3) were considered and it was concluded that

[the ALRC] maintains the view that the archives legislation provides adequate protection for such of these records as may survive to the open period. However, ... it remains a matter for Parliament to determine whether non-disclosure provisions in other legislation should apply to open period records. Rather than including a provision such as section 33(3) in the archives legislation, the Commission considers that any perceived need for added protection of information provided to the Australian Taxation Office or the Australian Bureau of Statistics in confidence should be addressed in a review of the relevant non-disclosure provisions in federal legislation,

---

169 National Archives of Australia, *Submission SR 29*, 23 February 2009.

170 Ibid.

171 Ibid.

followed, if appropriate, by amendment of that legislation to clearly indicate that the non-disclosure provisions apply to records in the open period.<sup>172</sup>

4.152 Taxation secrecy provisions have been reviewed recently<sup>173</sup> and are the subject of an exposure draft bill—Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Tax Laws Exposure Draft Bill). The object as set out in the Explanatory Material is ‘to consolidate and standardise’ the various secrecy provisions into a new framework, the ‘key principle’ of which is the protection of taxpayer information and to provide ‘clarity and certainty’ to taxpayers, the ATO and users of taxpayer information.<sup>174</sup> The new framework gives effect to the primary objective of protecting the confidentiality of taxpayer information

by placing a general prohibition on the disclosure of taxpayer information. However, in recognition of the importance that taxpayer information can play in facilitating efficient and effective government administration and law enforcement, disclosure of taxpayer information [is] permitted in certain specified circumstances. As a guide for future policy consideration, the disclosure of taxpayer information should be permitted only where the public benefit associated with the disclosure clearly outweighs taxpayer privacy.<sup>175</sup>

4.153 There is no proposed provision for any amendment to the *Archives Act*, nor was there discussion of taxpayer information in the open access period.

4.154 The emphasis in the ALRC’s recommendations in ALRC 85 was to complement the idea of access that underpins the introduction of both the *Archives Act* and the FOI Act. The range of exempt records was recommended to be reduced, and that where exemptions were to be claimed, the damage, prejudice or adverse effect of release relied upon ‘must be real and substantial’.<sup>176</sup>

4.155 The comments in the Explanatory Material to the Tax Laws Exposure Draft Bill reflect a similar approach. Although the emphasis is on the maintenance of the confidentiality of the records, disclosure is permitted ‘where the public benefit associated with the disclosure clearly outweighs taxpayer privacy’. Such an approach can be seen to be consistent with the recommendation in ALRC 85 to focus claims for exemption onto questions of harm. So, for example, if s 33(3) was repealed, a claim for access to a taxpayer’s information in the open access period would be assessed against the other exemptions, such as that it would involve ‘the unreasonable disclosure of information relating to the personal affairs’ of a person.<sup>177</sup>

---

172 Australian Law Reform Commission, *Australia’s Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), [20.79]

173 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006).

174 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), 3.

175 Ibid, [1.16]

176 Australian Law Reform Commission, *Australia’s Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Rec 155.

177 *Archives Act 1983* (Cth) s 33(g).

4.156 The ALRC is of the view that the recommendation made in ALRC 85 for the repeal of s 33(3) should be affirmed.

#### ***Clarifying provision?***

4.157 Secrecy provisions as considered throughout this Discussion Paper occur in many forms. Many impose direct obligations of non-disclosure—like the one contained in the *Archives Act* with respect to census information. Others are in the nature of codes, indicating when information may be disclosed.<sup>178</sup>

4.158 When records are transferred to the custody of the NAA, the Archives officers have obligations, as Commonwealth officers, in relation to those records. But when can the broad obligations of non-disclosure be said to override an access claim in the open period?

4.159 Given that the NAA has raised this as an important issue requiring clarification, the ALRC is of the view that such a provision should be introduced into the *Archives Act*. There is already a clear analogy in s 59 with respect to security classifications. They cease to have effect and the availability of any record to be released in the open access period must be considered against the other exemption provisions. This provides a principled basis for review of a claim for access at the relevant time.

4.160 The recommendation in ALRC 85 was to similar effect: for the amendment of the *Archives Act* to provide expressly that non-disclosure provisions in other legislation do not override the public access provisions of the archives legislation. The recommendation also contained a rider—‘unless this is expressly provided for in the legislation concerned’.<sup>179</sup> This allowed for the argument that there may be compelling reasons for the protection of essential public interests that are not identified in the exempt records categories and, in such a case, this should be made clear in the relevant legislation.

**Proposal 4–5** Complementing the idea of access that underpins both the *Archives Act 1983* (Cth) and the *Freedom of Information Act 1982* (Cth), s 33(3) of the *Archives Act* should be repealed.

**Proposal 4–6** The *Archives Act 1983* (Cth) should be amended to include a provision modelled on s 59, to the effect that where a record enters the open access period, any non-disclosure provision applicable to the record ceases to have effect, unless expressly stated in the relevant legislation.

<sup>178</sup> For example, *Trade Practices Act 1974* (Cth) s 89.

<sup>179</sup> Australian Law Reform Commission, *Australia’s Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Rec 108.

**Proposal 4–7** The Office of Parliamentary Counsel should issue a Drafting Direction that any proposed non-disclosure provision should indicate expressly whether it overrides the *Archives Act 1983* (Cth) in the open access period.

## Privacy

### Overview of the *Privacy Act 1988* (Cth)

4.161 The *Privacy Act 1988* (Cth) aims to protect personal information about individuals and give them some control over how that information is collected, stored, used and disclosed. It also gives individuals rights of access to, and correction of, their own personal information.<sup>180</sup> The *Privacy Act* focuses on the information and its management and does not impose penalties on Commonwealth officers for mishandling it—such matters being the concern of secrecy laws.

4.162 The *Privacy Act* contains safeguards set out in a number of Information Privacy Principles (IPPs) and National Privacy Principles (NPPs), which have the force of law.<sup>181</sup>

4.163 The IPPs cover ‘personal information’ which is collected or in a ‘record’ held by an ‘agency’, as those terms are defined in the *Privacy Act*. With limited exceptions, these agencies include only Australian Government and ACT public sector entities.<sup>182</sup> The NPPs cover personal information collected or held in a record by certain private sector organisations.<sup>183</sup> ‘Organisation’ is defined as an individual, a body corporate, a partnership, any other unincorporated association or a trust.<sup>184</sup> The *Privacy Act* applies to ‘acts and practices’; that is, acts done and practices engaged in by agencies or organisations.

<sup>180</sup> The ALRC recently conducted a major inquiry into Australian privacy laws: see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008).

<sup>181</sup> *Privacy Act 1988* (Cth) s 14 (IPPs), sch 3 (NPPs).

<sup>182</sup> Ibid s 6(1) defines ‘agency’ to include ministers, departments, federal courts and other bodies established for a public purpose.

<sup>183</sup> The *Privacy Amendment (Private Sector) Act 2000* (Cth) came into operation on 21 December 2001 and extended the coverage of the *Privacy Act* to much of the private sector. The private sector provisions of the *Privacy Act* apply to ‘organisations’. An individual who is self-employed or a sole trader is considered an organisation for the purposes of the *Privacy Act*. Organisations are generally responsible for the actions of their employees, contractors and subcontractors, all of which are covered by the *Privacy Act*: ss 6C, 8. In Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), the ALRC recommended that there should be a unified set of privacy principles that regulates both agencies and organisations: Rec 18–2.

<sup>184</sup> *Privacy Act 1988* (Cth) s 6C.

4.164 ‘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.<sup>185</sup>

4.165 Personal information includes written or electronic records about individuals, such as social security records and medical 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 may also fall within the definition of personal information because the context provides information, possibly sensitive personal information, about the individual.

4.166 ‘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 or genetic information about an individual, or information or an opinion about an individual, including that individual’s racial or ethnic origin, political opinions, religious beliefs or affiliations or sexual preferences or practices.<sup>186</sup>

4.167 The *Privacy Act* contains a range of exemptions and exceptions, which are found throughout the Act, in the definition of some terms, in specific exemption provisions and in the IPPs and NPPs themselves. The acts and practices of some Australian Government agencies—including the intelligence agencies ASIS, ASIO and ONA—are completely exempt from the *Privacy Act*.<sup>187</sup>

4.168 While information that is subject to secrecy provisions is generally handled by a government agency and is therefore subject to the IPPs, some secrecy provisions regulate organisations that ‘stand in the shoes’ of a Commonwealth officer, or secondary disclosures to other organisations, which may then be covered by the NPPs.

4.169 The Federal Privacy Commissioner has a number of statutory functions in relation to handling complaints, investigating breaches, and enforcing the *Privacy Act*.<sup>188</sup> Under pt V of the Act, the Commissioner has the power to investigate complaints,<sup>189</sup> obtain information and documents<sup>190</sup> and examine witnesses.<sup>190</sup> The Commissioner’s

---

<sup>185</sup> Ibid s 6(1). In ALRC 108, the ALRC recommended that the *Privacy Act* should define ‘personal information’ as ‘information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual’: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 6–1.

<sup>186</sup> *Privacy Act 1988* (Cth) s 6(1).

<sup>187</sup> Ibid s 7. In ALRC 108, the ALRC expressed the view that the current exemptions that apply to the intelligence and defence intelligence agencies under the *Privacy Act* should remain: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [34.94]–[34.109].

<sup>188</sup> *Privacy Act 1988* (Cth) s 40.

<sup>189</sup> Ibid s 44.

<sup>190</sup> Ibid s 45.

determinations may be enforced by proceedings in the Federal Court of Australia or the Federal Magistrates Court.<sup>191</sup>

4.170 The FOI Act and the *Privacy Act* both include provisions concerning access to personal information. As noted in the *Companion Guide* to the FOI Exposure Draft Bill:

The vast majority of FOI requests are submitted by applicants seeking access to their own information. While the Privacy Act 1988 regulates the collection, handling, access and disclosure of personal information, access to and correction of a person's own information is enforced through the FOI Act.<sup>192</sup>

4.171 As further noted, in order to provide greater clarity of the operation of each Act in relation to personal information, '[t]he Government proposes to amend the Privacy Act to enact an enforceable right of access to, and correction of, an individual's own personal information, rather than maintain this right through the FOI Act'.<sup>193</sup> Such amendments will be included in an exposure draft Bill to implement recommendations in the ALRC's 2008 Report, *For Your Information: Australian Privacy Law and Practice* (ALRC 108).

This will make the Privacy Act the key Commonwealth law for the collection, handling, disclosure and access to personal information. The co-location of privacy and FOI in a single office, and the future reform to the Privacy Act ... is intended to strengthen and elevate the role and importance of privacy laws.<sup>194</sup>

## Privacy and secrecy

4.172 The *Privacy Act* addresses specific secrecy provisions in pt VIA.<sup>195</sup> This part makes special provision for the collection, use and disclosure of personal information in emergencies or disasters. Section 80P(1) provides that when an emergency declaration is in force, an entity may collect, use or disclose personal information in certain circumstances. Section 80P(2) provides that an entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by s 80P(1), unless the secrecy provision is a 'designated secrecy provision'. Designated secrecy provisions include provisions under the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth).<sup>196</sup>

---

191 Ibid s 55A.

192 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009), 14.

193 Ibid.

194 Ibid.

195 The *Privacy Act* was amended in 2006 to insert this Part: *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth). The Part commenced operation on 7 December 2006.

196 *Privacy Act 1988* (Cth) s 80P(7).

4.173 In ALRC 108, the ALRC considered whether secrecy provisions in federal legislation contribute to inconsistency and fragmentation in the regulation of personal information. The ALRC also considered whether there is a need to clarify the relationship between the *Privacy Act* and other legislation containing secrecy provisions. Unfortunately, relatively few stakeholders made submissions on these issues.<sup>197</sup>

4.174 The ALRC concluded that, for a number of reasons, it is appropriate that specific laws, rather than the *Privacy Act*, include secrecy provisions designed to protect information. First, inserting criminal offences into the *Privacy Act* would be inconsistent with the ‘light touch’ regulatory regime for privacy. It would not be appropriate for the privacy regulator, the Federal Privacy Commissioner, to administer and enforce secrecy provisions.<sup>198</sup> Secondly, as discussed in Chapter 2 of ALRC 108:

Secrecy provisions do not relate solely to personal information. They also protect, for example, commercial, security and operational information. Secrecy provisions provide separate and specific standards of protection beyond those afforded by the privacy principles ... Unlike the privacy principles, the level of protection afforded by secrecy provisions will often vary with the sensitivity of the information concerned.<sup>199</sup>

4.175 Given that secrecy provisions may adversely affect the privacy of an individual, however, the ALRC suggested that a privacy impact assessment should be prepared when a secrecy provision is proposed that may have a significant impact on the handling of personal information. Further, the ALRC suggested that where a secrecy provision regulates personal information, that provision should address how the requirements under the provision interact with the privacy principles in the *Privacy Act*.<sup>200</sup>

### *Access and correction*

4.176 As noted above, the *Privacy Act* provides individuals with access and correction rights for personal information that relates to them, unless denying access is required or authorised by or under law.<sup>201</sup> If secrecy provisions should regulate personal information, there may be an issue whether they should restrict disclosure of that information to the individual about whom the information relates.

---

197 Nearly 600 submissions were received over the course of the ALRC’s Privacy Inquiry. Only 6 stakeholders commented on secrecy in response to the Issues Paper: Australian Law Reform Commission, *Review of Privacy*, Issues Paper 31 (2006). No stakeholder addressed the issue in response to Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007). Those stakeholders that commented on the earlier stages were: Department of Employment and Workplace Relations, Australian Bureau of Statistics, the Department of Health and Ageing, Office of the Victorian Privacy Commissioner, Office of the Privacy Commissioner and the Australian Privacy Foundation. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [15.116].

198 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [15.117]–[15.118].

199 *Ibid*, [15.121].

200 *Ibid*, [15.122]–[15.124].

201 *Privacy Act 1988* (Cth) s 14, IPP 6; sch 3, NPP 6.1(h).

4.177 Currently, secrecy provisions take various approaches to this issue. Section 86–2 of the *Aged Care Act 1997* (Cth) creates an offence for the unauthorised handling of ‘protected information’ acquired by the person in the course of performing duties or exercising powers or functions under the Act. However, the section contains an exception for information disclosed ‘only to the person to whom it relates’.<sup>202</sup>

4.178 Section 94 of the *Australian Trade Commission Act 1985* (Cth) restricts the disclosure of information by a person, to any person, of ‘any information concerning the affairs of another person acquired by the first-mentioned person by reason of his or her employment’. While this provision does not contain an exception that expressly allows the disclosure of information to an individual to whom the information relates, it appears from the wording of the provision that such disclosure would be permitted.

4.179 In contrast, s 44 of the *Surveillance Devices Act 2004* (Cth) does not allow the disclosure to an individual of personal information about that individual. This section creates two offences for the disclosure of ‘protected information’.<sup>203</sup> Protected information is defined to include ‘any information that is likely to enable the identification of a person, object or premises specified in a warrant’. This could include personal information. Section 44 sets out a number of exceptions to these offences—however, there is no exception that is equivalent to that contained in s 86–2 of the *Aged Care Act*.

### **Facilitating disclosure?**

4.180 The *Privacy Act* and some secrecy provisions place restrictions around the handling of personal information. However, there may be an issue where a secrecy provision facilitates disclosure of personal information by triggering exceptions in the privacy principles. This could occur if a secrecy provision contains an exception to the prohibition on disclosure. Exceptions in secrecy provisions often mirror the exceptions set out in the privacy principles. However, if a secrecy provision contains an exception that is not contained in the privacy principles, this could allow disclosure of personal information that would otherwise be a breach of the privacy principles.

4.181 Such an exception in a secrecy provision would be consistent with the *Privacy Act* because it could fall within two types of exceptions in the privacy principles. First, use and disclosure is permitted under the privacy principles if this is ‘required or authorised by or under law’.<sup>204</sup> Secondly, use and disclosure is also permitted under the privacy principles if this is ‘reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue’.<sup>205</sup>

---

202 *Aged Care Act 1997* (Cth) s 86-2(2)(b).

203 *Surveillance Devices Act 2004* (Cth) s 44(3) also prohibits the admission of protected information in evidence in any proceedings.

204 *Privacy Act 1988* (Cth) s 14, IPPs 10.1(c) and 11.1(d); sch 3, NPP 2.1(g).

205 *Ibid* s 14, IPPs 10.1(d) and 11.1(e); sch 3, NPP 2.1(h).

## Submissions

4.182 In IP 34, the ALRC asked a number of questions concerning the relationship between secrecy provisions and the *Privacy Act*.<sup>206</sup>

4.183 The differences between privacy and secrecy were remarked upon by a number of commentators.<sup>207</sup> In the AGD's submission, for example, privacy and secrecy were described as 'distinct areas of the law':

Privacy law is primarily aimed at protecting the rights of individuals to privacy, while secrecy laws are intended to prevent unauthorised disclosure of sensitive information. Some overlap does exist where secrecy laws deal with similar types of information to that regulated by the *Privacy Act*. In particular, secrecy laws may regulate the same information where it is considered appropriate to impose criminal sanctions for unauthorised disclosure of personal information (which may or may not be broader than the information covered by the *Privacy Act*). As the Taxation Secrecy Discussion Paper noted, criminal sanctions provide an important deterrent and provide a strong message that unauthorised use and disclosure of personal information will not be tolerated. Remedies available under the *Privacy Act*, which include making a complaint to the Privacy Commissioner and requiring the agency to compensate any loss, arguably do not have the same deterrent effect for individual officers.<sup>208</sup>

4.184 The distinct, yet overlapping nature of the two areas was also remarked upon by the DHS:

the Privacy Act and secrecy laws work together in relation to personal information (information about a living identifiable individual). Generally personal information falls within the various definitions of protected information. ...

Where information is regulated by both the Privacy Act and secrecy laws, then both sets of provisions must be satisfied. For example, collection and use within Centrelink must be consistent both with Information Privacy Principles (IPPs) 1-3 and 10 in s 14 of the Privacy Act and any relevant secrecy provision. In circumstances where use is authorised under a secrecy provision, it would be expected to satisfy the current tests of relevance and necessity in the IPPs.

In relation to disclosure, the Department understands that in general terms a disclosure which is authorised under a secrecy provision will be authorised by law, and therefore permitted under IPP 11.1(d) in s 14 of the Privacy Act. However, not all provisions are clear on this point. For example, the Centrelink provisions contain explicit authorisations for various dealings (see, s 202 of the Social Security (Administration) Act) but there is a question whether very broad provisions permitting disclosure 'in the performance of duties' are sufficiently precise to enliven IPP 11.1(d). It is important that agencies remain able to undertake data matching activities within the agency and with other agencies, particularly in relation to

<sup>206</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Questions 7–4 to 7–5.

<sup>207</sup> Attorney-General's Department, *Submission SR 36*, 6 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; I Turnbull, *Submission SR 15*, 17 February 2009.

<sup>208</sup> Attorney-General's Department, *Submission SR 36*, 6 March 2009. See also Australian Press Council, *Submission SR 16*, 18 February 2009.

identifying circumstances of fraud or over- or under- provision of services and benefits.

In relation to access and correction, both the Privacy and FOI Acts allow individuals an opportunity to access and seek correction of their personal information. Human services agencies are amongst the most common recipients of applications for amendment. No barriers to these processes arising from the current secrecy laws were identified in discussions with portfolio agencies.<sup>209</sup>

4.185 The ARTK coalition acknowledged that neither secrecy nor privacy were sufficient of themselves to deal with issues concerning the protection of personal information:

Given that there are likely to be many circumstances where official information, subject to secrecy obligations, will also constitute personal information for the purposes of the *Privacy Act 1988* (Cth), it does not appear feasible to seek to regulate personal information either exclusively through secrecy laws or exclusively under the Privacy Act. However, privacy should not be used [as] a shroud to the provision of information to the public. It is the experience of the members of the ARTK that government departments often make such a claim to avoid disclosure of information that can or should be made public.<sup>210</sup>

4.186 The latter concern was also evident in the Privacy Inquiry, where it was described as the ‘BOTPA’ (because of the *Privacy Act*) response.<sup>211</sup> Dr Ian Turnbull suggested that there is a confusion between the concepts, and that:

‘Privacy’ protection should be under the Privacy legislation ... partly to separate it from ‘secret’ information. ...

Secrecy provisions should regulate personal information where that information (primarily identifying information) has become or been made secret. Examples are unlisted or secret telephone numbers, or addresses of protected witnesses or domestic violence victims.

By way of examples, two FOI requests were rejected under the ‘privacy’ exemption of the Victorian legislation. Both demonstrated a failure to distinguish ‘private’ from ‘secret’. Both rejections effectively prevented scrutiny of public authority actions.<sup>212</sup>

4.187 The ATO commented that the *Privacy Act* ‘would not, of itself, provide sufficient protection for the confidentiality of taxpayer information’:

The ATO considers that the Privacy Act provides an appropriate mechanism for allowing individuals to access and correct information about themselves, and that it is unnecessary for secrecy provisions to duplicate the Privacy Act in this regard. Further, tax secrecy provisions will never apply to restrict a taxpayer from accessing his or her own tax information.<sup>213</sup>

---

209 Department of Human Services, *Submission SR 26*, 20 February 2009.

210 Australia’s Right to Know, *Submission SR 35*, 6 March 2009.

211 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), 109.

212 I Turnbull, *Submission SR 15*, 17 February 2009.

213 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

4.188 With respect to the question of whether similar terminology should be used in both areas, the DHS commented that:

[S]ecrecy provisions apply to a wider range of information than the *Privacy Act* does. This suggests that adopting *Privacy Act* terminology would not be appropriate (absent an intention to restrict the coverage of secrecy laws to be coterminous with the *Privacy Act*).<sup>214</sup>

4.189 The Social Security Appeals Tribunal (SSAT) agreed that consistent terminology would be useful, given that the ‘plethora of provisions and definitions give rise to a great deal of confusion and difficulty of application’:

The SSAT, therefore, welcomes the adoption of consistent terminology throughout Commonwealth legislation so that information is uniformly described in line with, for example, the definition of ‘personal information’ in the *Privacy Act*.<sup>215</sup>

4.190 The AGD suggested, however, that:

It may be helpful if secrecy provisions that regulate personal information as defined in the *Privacy Act* used the same terminology for consistency. Terms such as ‘affairs of a person’ have the potential to cause uncertainty as to their scope, because section 22 of the *Acts Interpretation Act 1901* provides that, unless the contrary intention appears, the term person includes bodies corporate and bodies politic. To avoid doubt, it would be helpful for secrecy provisions using the term ‘person’ to clarify whether it is intended to only mean a natural person or whether it has the broader meaning given by the *Acts Interpretation Act*.<sup>216</sup>

4.191 Similarly, the Department of Education, Employment and Workplace Relations (DEEWR) commented that:

there may be some benefit in consistency of terminology between the *Privacy Act* and the secrecy provisions. For example, the distinction between use and disclosure. However, there would seem to be little value in a secrecy provision simply mirroring the *Privacy Act*, if it is accepted that legislation specific secrecy provisions are designed to cater for the particular context and nature of the information being regulated.<sup>217</sup>

4.192 The submission from DEEWR also emphasised the importance of ‘quality training’ to ensure that staff clearly understood the interaction between secrecy provisions and the *Privacy Act* and that contractors were aware of their privacy obligations.<sup>218</sup>

---

<sup>214</sup> Department of Human Services, *Submission SR 26*, 20 February 2009.

<sup>215</sup> Social Security Appeals Tribunal, *Submission SR 14*, 17 February 2009.

<sup>216</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

<sup>217</sup> Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

<sup>218</sup> Ibid.

4.193 The AGD also submitted that there may be legitimate reasons for authorising the handling of personal information via secrecy provisions, such as ‘law enforcement or the detection and prevention of fraud’.<sup>219</sup>

### **ALRC’s views**

4.194 It is evident that there is much confusion in the public arena about what is a privacy matter and what is governed by secrecy provisions. The interaction of secrecy provisions and personal information is considered throughout this Discussion Paper.

---

219 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.



## 5. Overview of Current Secrecy Laws

---

### Contents

Introduction	153
Common law duties	154
Breach of confidence	154
Duty of fidelity and loyalty	155
Sufficiency of the common law	158
Statutory secrecy provisions	161
What kind of information is protected?	162
Whose activity is regulated?	172
What kind of activity is regulated?	176
Method of regulation	177
Exceptions and defences	178
General criminal offences	184
Section 70—disclosure of information by Commonwealth officers	185
Section 79—disclosure of official secrets	191
Comment	196

### Introduction

5.1 The way that individuals use and disclose government information is subject to several layers of regulation. Previous chapters have examined the handling of government information in the context of other laws, such as freedom of information and privacy laws, and the broader principles of open government. This chapter provides a broad overview of the laws that currently regulate the use and disclosure of government information by individual persons and agencies.

5.2 First, the equitable and common law duties of confidentiality, loyalty and fidelity that apply to some aspects of using and disclosing government information are considered. Secondly, this chapter examines statutory secrecy provisions currently contained in Commonwealth legislation. In particular, this chapter sets out the common elements of statutory secrecy provisions and identifies points of difference and variation among them. Finally, overlaying this array of common law and statutory duties are the general criminal offences in ss 70 and 79 of the *Crimes Act 1914* (Cth), which apply criminal sanctions to the breach of secrecy obligations.

## Common law duties

### Breach of confidence

5.3 The equitable action for breach of confidence may be used to restrict the disclosure of information in certain circumstances. In the High Court case of *Commonwealth v Fairfax*,<sup>1</sup> Mason J cited with approval the following formulation of the law:

The principle is that the court will ‘restrain the publication of confidential information improperly or surreptitiously obtained or of information imparted in confidence which ought not to be divulged’.<sup>2</sup>

5.4 An action can also be brought against a third party to whom information has been communicated in breach of a duty of confidence where that third party was aware, or should reasonably have been aware, that the information was confidential.

5.5 *Commonwealth v Fairfax* gave rise to the question of the applicability of the doctrine of breach of confidence in the context of disclosure of government information and the availability of an injunction in such a case. *The Age* and *The Sydney Morning Herald* newspapers were proposing to publish extracts from an upcoming book, *Documents on Australian Defence and Foreign Policy 1968–1975*,<sup>3</sup> including parts of classified government documents dealing with the ANZUS Treaty and the East Timor crisis. Copies of the early editions of the newspapers had been distributed before the publishers received notice of the interim injunction restraining publication. Mason J concluded that the information had probably been leaked by a public servant in breach of his or her duty and contrary to the security classifications marked on some of the documents.

5.6 Mason J commented that, although the equitable action for breach of confidence was developed ‘to protect the personal, private and proprietary interests of the citizen, not to protect the very different interests of the executive government’,<sup>4</sup> he accepted that in some circumstances the principles of breach of confidence could be applied to protect information in the hands of government. To do so, however, it must be shown

not only that the information is confidential in quality and that it was imparted so as to import an obligation of confidence, but also that there will be ‘an unauthorised use of that information to the detriment of the party communicating it’. The question then, when the executive government seeks the protection given by equity, is: What detriment does it need to show?<sup>5</sup>

<sup>1</sup> *Commonwealth v Fairfax* (1980) 147 CLR 39.

<sup>2</sup> *Ibid*, 50, citing Swinfen Eady LJ in *Lord Ashburton v Pope* (1913) 2 Ch 469, 475.

<sup>3</sup> G Munster and J Walsh, *Documents on Australian Defence and Foreign Policy 1968–1975* (1980).

<sup>4</sup> *Commonwealth v Fairfax* (1980) 147 CLR 39, 51.

<sup>5</sup> *Ibid*, notes omitted.

5.7 The conclusion drawn in the case was that disclosure of confidential information would be restrained at the instance of the government if it appeared that disclosure would be ‘inimical to the public interest because national security, relations with foreign countries or the ordinary course of business of government will be prejudiced’. Mason J noted that:

it can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticize government action.

Accordingly, the court will determine the government’s claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.<sup>6</sup>

5.8 The High Court reiterated the importance of public discussion in *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd (No 2)*,<sup>7</sup> where it referred to the ‘public interest in freedom of information and discussion’.<sup>8</sup> Such an emphasis is also consistent with the philosophy of the *Freedom of Information Act 1982* (Cth) considered in Chapter 4.

5.9 The duty of confidentiality may also have application in circumstances where the government has a contractual relationship with a private provider of a government service (for example, a provider of an aged care service).<sup>9</sup> The obligation of confidence may arise because of the circumstances in which the information is imparted or because of an express contractual stipulation. Confidentiality clauses are now included in many government contracts with service providers as a matter of course.<sup>9</sup> This is considered further in Chapter 14.

5.10 Information held by government contractors that is appropriately categorised as ‘commercial in confidence’, subject to a confidentiality clause, or subject to restraint from publication by the equitable duty of confidence, may therefore be subject to a particular level of protection by virtue of obligations of confidence, in addition to whatever legislative secrecy provisions may apply in the circumstances.

### Duty of fidelity and loyalty

5.11 The common law imposes on any employee the duty of fidelity and loyalty (or good faith). This duty arises from the contract of employment,<sup>10</sup> but may also arise

6 Ibid, 52.

7 *Attorney-General (UK) v Heinemann Publishing Australia Pty Ltd (No 2)* (1988) 165 CLR 30, 45.

8 J Macken, P O’Grady, C Sappideen and G Warburton, *Law of Employment* (4th ed, 2002), 141.

9 Australian Parliament—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), 53.

10 *Robb v Green* [1895] 2 QB 315.

from a fiduciary obligation where the employee is in a special position of trust and confidence.<sup>11</sup> The duty of fidelity has largely been imposed in situations involving confidential information and has been expressed as meaning that an employee must not use information obtained in the course of his or her employment to the detriment of the employer.<sup>12</sup>

5.12 In his report, *Integrity in Government: Official Information*, Paul Finn noted that the effect of the duty of fidelity on a public servant is more complicated than in the case of a private sector employee, as public servants have a duty to their employer as well as an overriding duty to the public at large.

For this reason, and as with the law of confidentiality as it applies to governmental information, the ‘public interest’ and not merely the ‘employer’s’ interests, can affect the incidents of the duty itself.<sup>13</sup>

5.13 Finn noted that the formulation of the duty is necessarily imprecise. This is because of the variety of considerations that must be brought to bear on the question of the propriety of the use, including:

the nature of the information and whether or not it is publicly available; the nature of the office held; the possible effects of allowing its use in the circumstances of its use; the actual or likely consequences of that use; and the public interests which might justify or deny the use.<sup>14</sup>

5.14 Some years later, in *Bennett v President, Human Rights and Equal Opportunity Commission*, Finn J made a number of comments about whether a direction not to disclose information could be supported by the public servant’s duty of fidelity and loyalty as an employee.<sup>15</sup> He noted that the features of the duty were dependent on the facts in each case, and that public sector employees may have different demands placed upon them by virtue of their position.

The difficulty this creates ... is that there is no significant Australian jurisprudence on how the duty is to be adapted to accommodate the distinctive demands of public service employment that result from the ‘special position’ ... public servants enjoy ... This is not the place to essay the significance that ought to be given to the precepts of loyalty, neutrality and impartiality which are hallmarks of a public service in a system of responsible government and which have been relied upon in other jurisdictions (most notably Canada) in justifying the imposition of restrictions on public servants in exercising freedom of expression. ... My only comment would be that to consider the duty ... without regard to such precepts would involve a flight from reality.<sup>16</sup>

---

11 J Macken, P O’Grady, C Sappideen and G Warburton, *Law of Employment* (4th ed, 2002), 139–141.

12 *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 625–628.

13 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 204.

14 *Ibid*, 205–206.

15 It should be noted that this issue was remitted back to the Human Rights and Equal Opportunity Commission: *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [128]–[129].

16 *Ibid*, [125].

5.15 Finn J referred to Canadian jurisprudence and particularly the conclusion of the Supreme Court of Canada in *Fraser v Public Service Staff Relations Board* ('*Fraser*') that, in relation to comments critical of the government, the Court must balance the right of an individual, as a member of the Canadian community, to speak freely on issues of public importance against the duty of that individual, as a public servant, to fulfil his or her functions as an employee of the government.<sup>17</sup> The Court held that some comments by public servants were permitted and would be appropriate in circumstances where:

- the government was engaged in illegal acts;
- the government's policies jeopardised the life, health or safety of persons; or
- the comments had no impact on the ability of the employee to perform his or her duties.<sup>18</sup>

5.16 However, the right to comment was not unqualified. Dickson CJ stated that:

Public servants have some freedom to criticize the Government. But it is not an absolute freedom. To take but one example, whereas it is obvious that it would not be 'just cause' for a provincial government to dismiss a provincial clerk who stood in a crowd on a Sunday afternoon to protest provincial day care policies, it is equally obvious that the same government would have just cause to dismiss the Deputy Minister for Social Services who spoke vigorously against the same policies at the same rally.<sup>19</sup>

5.17 In the later cases of *Osborne v Canada*<sup>20</sup> and *Haydon v Canada*,<sup>21</sup> the Canadian Courts further considered the ability of public servants to comment on government matters in the context of the right of freedom of speech under the *Canadian Charter of Rights and Freedoms*. In common with most human rights charters internationally, s 1 of the Canadian Charter guarantees the rights and freedoms set out in it, subject to 'such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society'.

5.18 In *Osborne v Canada*, the Supreme Court followed the reasoning in *Fraser*, stating that restrictions on the rights of public servants to comment on government matters should be based on the level of seniority of the employee, including whether he or she participated in policy development or managerial decisions. This distinction allowed most public servants to participate freely in public discourse, while still maintaining the neutrality of the public service overall.<sup>22</sup>

---

17     *Fraser v Public Service Staff Relations Board* [1985] 2 SCR 455, [34].

18     *Ibid*, [41].

19     *Ibid*, [36].

20     *Osborne v Canada* [1991] 2 SCR 69.

21     *Haydon v Canada* [2001] 2 FC 82.

22     *Osborne v Canada* [1991] 2 SCR 69, 99.

5.19 In *Haydon v Canada*, the Federal Court held that the common law duty of fidelity and loyalty provided a reasonable limit on freedom of expression within the Charter and cited with approval the three exceptions outlined in *Fraser*, above, where disclosure or comment would be allowed. In *Haydon v Canada*, the disclosures related to drug approval processes for bovine growth hormones. The Court found that the issue of the safety of growth hormones was ‘a legitimate public concern requiring a public debate’ and that ‘the common law duty of loyalty does not impose unquestioning silence’.<sup>23</sup> It was also an important feature of that case that attempts had been made to resolve the issues internally before public comments were made.

5.20 In *Read v Canada*,<sup>24</sup> the Federal Court acknowledged that while there could be other specific exceptions to the duty in addition to those enunciated in *Fraser*, there was no generalised ‘public interest’ exemption. Harrington J rejected the proposition that *Haydon v Canada* had created a more general exception, finding that the public concern in that case was specifically a danger to the health and safety of persons and therefore within the exceptions identified in *Fraser*.<sup>25</sup>

### Sufficiency of the common law

5.21 Christopher Erskine SC has suggested that the Canadian cases set out a principled basis upon which a balancing process can be undertaken to determine when the right of a public servant to comment outweighs their duty to the effective functioning of government.<sup>26</sup> He considers that the common law duty of fidelity ‘has coherent and sensible principles that neatly cover the difficult questions raised by public servants disclosing information’.<sup>27</sup>

5.22 Are these principles applicable in the Australian context, particularly given the absence of an Australian federal equivalent to the *Canadian Charter of Rights and Freedoms*? As Finn J noted in *Bennett*, there is little law on how the duty of fidelity applies to public servants in Australia. If the Canadian principles were applied, there is a question whether the duty under reg 2.1 of the *Public Service Regulations 1999* (Cth) and the consequent general offence under s 70 of the *Crimes Act* are necessary. Would the common law principles cover the field to provide sufficient protection of Commonwealth information?

5.23 Erskine outlines a number of reasons why the common law framework might be preferable to the duty imposed by the regulation or other statutory provisions, including that:

---

23     *Haydon v Canada* [2001] 2 FC 82, [120].

24     *Read v Canada* [2005] FC 798.

25     Ibid, [107]–[108].

26     C Erskine, ‘The Bennett Decision Explained: The Sky is not Falling!’ (2005) 46 *Australian Institute of Administrative Law (AIAL) Forum* 15, 24.

27     Ibid, 15.

- the duty of fidelity is compatible with the implied freedom of political expression, as it is based on a ‘reasonableness test’,<sup>28</sup>
- the duty is not absolute but is tailored to what is fair in the circumstances of each case, thereby allowing the imposition of a higher duty where, for example, the public servant is a senior officer or where the information concerns matters of national security; and
- the duty does not prevent disclosure on matters of public health and safety or illegality.

5.24 Erskine suggests that, as a general rule, a public servant should raise concerns internally before making public comment. This would provide some protection for ‘whistleblowers’.<sup>29</sup>

### ***Submissions***

5.25 In the Issues Paper, *Review of Secrecy Laws* (IP 34), the ALRC asked whether the common law principles are appropriate and sufficient of themselves to regulate disclosure of Commonwealth information by public servants.<sup>30</sup>

5.26 Whistleblowers Australia responded by expressing the view that:

it is a waste of time addressing problems about secrecy and confidentiality legislation if it is possible to impose similar restrictions on disclosures by other practices or means. The common law facility of employee’s fidelity and loyalty and the utilisation of Client Legal Privilege are practices both of which are able to be used to prevent proper and appropriate disclosures of information.

The Commission will have failed to meet the terms of reference, if they consider statute law in respect of secrecy and confidentiality, while leaving unaddressed other means by which the public can be denied information to which it is entitled.<sup>31</sup>

5.27 Whistleblowers Australia further suggested that the common law duty of fidelity and loyalty is used as a tool to impose secrecy:

Regardless of any legislation or statute that provides agencies with the power to keep matters secret or confidential, the use or misuse of the common law power to impose fidelity and loyalty conditions is a significant impediment to employees to engage in the rightful and proper disclosure of information in the public interest.

Through the misuse of fidelity and loyalty provisions, agencies can impose severe and harsh penalties/damages on an employee for making adverse comments about the conduct of that agency.

---

28 The implied freedom of political communication issue is discussed further in Ch 2.

29 C Erskine, ‘The Bennett Decision Explained: The Sky is not Falling!’ (2005) 46 *Australian Institute of Administrative Law (AIAL) Forum* 15, 24–25. Public interest disclosures, or ‘whistleblowing’, is discussed further in Chs 9 and 11.

30 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 1–1.

31 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

It would not be sufficient to legislate to prevent criminal or civil action being taken against a person who properly and legitimately discloses particular information, if the door is left open for an agency to take industrial action against an employee for breaches of fidelity and loyalty.

It is essential that any legislation providing for appropriate disclosure of public interest information is not thwarted or undermined by the application of the common law impediments concerning employee fidelity and loyalty.<sup>32</sup>

5.28 The Australian Intelligence Community (AIC), however, submitted that general law obligations would be insufficient to protect Commonwealth information:

Secrecy laws themselves are essential to the effective operation of Australia's intelligence agencies; these agencies would not be able to operate effectively if secrecy laws were repealed or significantly diminished. A statutory duty on Commonwealth officers not to disclose information is fundamental to the operation of AIC agencies ... General law principles should not govern secrecy because that would allow for uncertainty regarding the scope and application of the law, which could ultimately inhibit national security.<sup>33</sup>

#### *ALRC's views*

5.29 The ALRC considers that a key outcome of this Inquiry should be clear and consistent secrecy provisions and an integration of public interest elements on a principled basis through the whole spectrum of information handling regulation in the Commonwealth sector. The inclusion of 'public interest disclosure' exceptions is a significant aspect of this and is considered in Chapters 9 and 11.

5.30 With respect to the argument by Whistleblowers Australia that this Inquiry should also consider the role of client legal privilege as a tool for suppressing public sector information,<sup>34</sup> the ALRC notes the role that the doctrine may have in limiting the disclosure of information obtained by way of legal advice or in relation to legal proceedings but does not propose in this Inquiry to examine the doctrine as a 'secrecy provision'. In this regard, the ALRC notes its 2007 Report, *Privilege in Perspective—Client Legal Privilege in Federal Investigations* (ALRC 107) and its 2005 Report, *Uniform Evidence Law* (ALRC 102) as well as the Terms of Reference, which focus upon legislative provisions regarding secrecy and confidentiality.

5.31 The ALRC is of the view that the general law obligations do not provide sufficient protection in the public sector context, and that it is necessary and desirable to have in place certain statutory provisions that impose obligations on Commonwealth officers and others who handle Commonwealth information.

---

32 Ibid.

33 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

34 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

## Statutory secrecy provisions

5.32 This section examines the numerous secrecy provisions contained in Commonwealth legislation.

5.33 As discussed in Chapter 1, the ALRC has conducted a mapping exercise to identify and analyse provisions in Commonwealth legislation that impose secrecy or confidentiality obligations on individuals or bodies in respect of the handling of Commonwealth information. The ALRC has identified 507 secrecy provisions in 175 pieces of primary and subordinate legislation. A table of secrecy provisions in Commonwealth legislation is set out in Appendix 4.

5.34 Approximately 70% of the statutory secrecy provisions identified create criminal offences. The remaining 30% of provisions set out a duty of confidentiality and establish rules for the handling of protected information and may specify civil or administrative penalties for breach. While the latter provisions are not, in themselves, offences, s 70 of the *Crimes Act* may attach criminal sanctions to the breach by a Commonwealth officer of this kind of ‘duty not to disclose’. In this way, specific secrecy provisions—that do not themselves create an offence—interact with general offences in the *Crimes Act* aimed at protecting confidential Commonwealth information.

5.35 Statutory secrecy provisions exhibit five common elements:

- protection of particular kinds of information;
- regulation of particular persons;
- prohibition of certain kinds of activities in relation to the information;
- methods of regulation, and, if a criminal offence, the elements of that offence; and
- exceptions and defences which set out the circumstances in which a person does not infringe a secrecy provision.

5.36 It is notable that this list of common elements of current secrecy provisions does not include an express ‘harm element’, such as a requirement that a disclosure of information is reasonably likely to cause harm to a specified public interest, or that a person, in disclosing the information, intended to cause harm. Only a small number of statutory secrecy offences expressly include a harm element. These provisions, and the desirability of including a harm element in secrecy offences, are discussed further in Chapter 10.

5.37 This section of the chapter examines each aspect of statutory secrecy provisions in turn and provides examples of the different approaches taken across Commonwealth legislation to the protection of official information. Where relevant, this section also notes the percentages of secrecy provisions that exhibit particular variations within the five elements outlined above. As this chapter provides an overview of all statutory secrecy provisions, the approximate values expressed here are different from figures noted in later chapters that focus on statutory secrecy offences alone.

### **What kind of information is protected?**

5.38 Secrecy provisions in Commonwealth legislation prohibit the unauthorised handling of a variety of information. This section examines such provisions according to the following categories:

- any information (or general secrecy provisions);
- information about the affairs of a person;
- taxation information;
- census and statistical information;
- electoral information;
- defence or security information;
- law enforcement and intelligence information;
- confidential information;
- Indigenous sacred or sensitive information; and
- other types of information.

#### ***Any information (or general secrecy provisions)***

5.39 Approximately 10% of secrecy provisions in Commonwealth legislation relate to the unauthorised disclosure or use of *any information* obtained by a person during the course of his or her employment.<sup>35</sup> Generally, these provisions prohibit the disclosure of any information obtained by a person carrying out, performing or exercising any of the person's duties, functions or powers under:

---

35 See, eg, *Australian Crime Commission Act 2002* (Cth) s 51(2); *Auditor-General Act 1997* (Cth) s 36(1); *Australian Hearing Services Act 1991* (Cth) s 67(1); *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15(1); *Australian Federal Police Act 1979* (Cth) s 60A(2); *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18(2), 81(1).

- the Act in which the provision is located;
- a particular part of the Act in which the provision is located;
- regulations made under the Act in which the provision is located; or
- another Act.

5.40 Australian Public Service (APS) employees have a general duty not to disclose official information. Section 13 of the *Public Service Act 1999* (Cth) sets out the APS Code of Conduct which requires an employee to behave honestly and with integrity in the course of his or her employment,<sup>36</sup> and to maintain appropriate confidentiality about dealings the employee has with any minister or minister's member of staff.<sup>37</sup>

5.41 Section 13(13) of the *Public Service Act* provides that an APS employee must also comply with any other conduct requirement prescribed by the regulations. Regulation 2.1(3) of the *Public Service Regulations* provides that:

an APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.<sup>38</sup>

5.42 Legislation establishing a statutory authority or independent agency may also include a similar general secrecy provision to cover the employees of that authority or agency.<sup>39</sup>

5.43 Section 70 of the *Crimes Act* covers a wide range of information in that it makes it an offence for a Commonwealth officer to disclose 'any fact or document' obtained by virtue of his or her position as a Commonwealth officer that it is 'his or her duty not to disclose'. Section 70 is discussed in more detail below.

#### ***Information about the affairs of a person***

5.44 A significant proportion of Commonwealth secrecy provisions (approximately 30%) aim to prevent the unauthorised use of information about individuals or persons.<sup>40</sup> The majority of these provisions refer to information about a 'person'. As

---

36 *Public Service Act 1999* (Cth) s 13(1).

37 *Ibid* s 13(6).

38 Reg 2.1 of the *Public Service Regulations 1999* (Cth) was amended in 2006, following the decision in *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334. The issues that arose for consideration in that case are discussed further in Ch 2. The text of reg 2.1 is set out in Appendix 5.

39 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 207(1); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 49(1); *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2).

40 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth), s 164(1); *Social Security (Administration) Act 1999* (Cth), s 204.

such, these provisions would also capture the disclosure of information about a body politic or corporate as well as a natural person.<sup>41</sup> However, some legislation refers to information relating to the affairs of an individual,<sup>42</sup> which refers to a natural person only.<sup>43</sup>

5.45 Some secrecy provisions that protect information of this type use the term ‘personal information’.<sup>44</sup> This is the term used in the *Privacy Act 1988* (Cth) and the *Freedom of Information Act*, which also regulate the disclosure of information about persons held by Australian Government agencies. Other laws refer to information ‘about a person’,<sup>45</sup> or ‘concerning another person’,<sup>46</sup> while a small number refer to ‘identifying information’,<sup>47</sup> or information that would enable people generally to ‘work out the identity of the individual to whom the information relates’.<sup>48</sup> The majority, however, refer to information about the ‘affairs’ of another person.

### **Taxation information**

5.46 A number of secrecy provisions aim to prevent the unauthorised disclosure of ‘taxation information’.<sup>49</sup> For the purposes of this discussion, ‘taxation information’ is defined as information provided by a taxpayer to a person or an agency pursuant to a legislative requirement contained in taxation legislation.

5.47 Secrecy provisions have long been used to protect the unauthorised disclosure of taxation information. The justification for the protection of taxation information is that it encourages voluntary compliance with taxation legislation.<sup>50</sup> It has been noted that ‘compliance with tax laws could be adversely affected if taxpayers thought their personal information could be disclosed easily’.<sup>51</sup> Secrecy provisions protecting

41 *Acts Interpretation Act 1901* (Cth) s 22.

42 See, eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 66; *Workplace Relations Act 1996* (Cth) ss 163C, 166T; *Health Insurance Regulations 1975* (Cth) reg 23C(2)(a).

43 *Acts Interpretation Act 1901* (Cth) s 22.

44 See, eg, *Higher Education Support Act 2003* (Cth) s 179-10; *Product Grants and Benefits Administration Act 2000* (Cth) s 47(2); *Aged Care Act 1997* (Cth) s 86-2(1).

45 See, eg, *Superannuation Contributions Tax (Assessment and Collection) Act 1997* (Cth) s 32(1), (2); *Superannuation Contributions Tax (Members of Constitutionally Protected Superannuation Funds) Assessment and Collection Act 1997* (Cth) s 28(1), (2); *Termination Payments (Assessment and Collection) Act 1997* (Cth) s 23(1), (2); *Superannuation Guarantee (Administration) Act 1992* (Cth) s 45(1), (2).

46 *Australian Institute of Health and Welfare Act 1987* (Cth) s 29(1).

47 See, eg, *Australian Citizenship Act 2007* (Cth) ss 42–43; *Migration Act 1958* (Cth) s 336E.

48 *Workplace Relations Act 1996* (Cth) ss 163C(1)(b), 166T(1)(b).

49 The Commonwealth Treasury has conducted a review of the various secrecy and disclosure provisions in Australian taxation laws and, in March 2009, released an exposure draft bill for public comment. The exposure draft bill proposes to consolidate the taxation secrecy and disclosure provisions currently found across 18 different statutes. See further, The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006); Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth).

50 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 1.

51 Ibid. This justification was considered in the context of the proposed repeal of *Freedom of Information Act 1982* (Cth) s 38 in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995). See also Ch 4.

taxation information almost always criminalise the unauthorised disclosure of the information.

5.48 Some of the secrecy provisions that protect taxation information specifically refer to the type of information protected. For example, s 8WB(1)(c) of the *Taxation Administration Act 1953* (Cth) prohibits the disclosure of a ‘tax file number’. However, most of the provisions prohibit the disclosure of information about a person that was disclosed or obtained under a piece of taxation legislation.<sup>52</sup> Some provisions also include the additional requirement that the information was obtained in the course of official employment.<sup>53</sup>

5.49 Further, a number of secrecy provisions that protect taxation information deal with the subsequent disclosure of the information. For example, s 3EA(2) of the *Taxation Administration Act* makes it an offence for an officer of the Australian Security Intelligence Organisation (ASIO) to disclose taxation information that he or she has obtained from the Commissioner of Taxation pursuant to s 3EA(1) of the Act.

### **Census and statistical information**

5.50 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).<sup>54</sup> The census is regarded as an important source of statistical information for use by governments, academics, businesses and private individuals. Section 19(1) of the *Census and Statistics Act* makes it an offence for any past or present officer of the ABS to disclose any information given under the Act otherwise than in accordance with a ministerial determination under s 13(1),<sup>55</sup> or for the purposes of the Act. Section 19(2) makes it an offence for a person to whom information has been disclosed pursuant to a determination under s 13(1) to fail to comply with an undertaking given in relation to the information. Section 19A of the Act provides that an officer of the ABS must not be required to disclose census information to an agency for 99 years following a census, unless the disclosure is in accordance with the Act.

5.51 Like taxation information, the justification for the protection of census information is that without the guarantee of secrecy, supported by criminal sanction, people may be reluctant to divulge sensitive personal information in the census.

<sup>52</sup> See, eg, *Inspector-General of Taxation Act 2003* (Cth) s 37(1), (2); *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 55(1); *Child Support (Assessment) Act 1989* (Cth) s 150(1), (2).

<sup>53</sup> See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30(1), (2); *Higher Education Funding Act 1988* (Cth) s 78(4); *Petroleum Resource Rent Tax Assessment Act 1987* (Cth) s 17(3); *Income Tax Assessment Act 1936* (Cth) s 16(2); *Excise Act 1901* (Cth) s 159(2).

<sup>54</sup> *Census and Statistics Act 1905* (Cth) s 8.

<sup>55</sup> Ibid s 13(1) provides that the Minister may, by legislative instrument, make determinations providing for and in relation to the disclosure of information (with the approval in writing of the Australian Statistician).

5.52 Census information may be transferred to the National Archives of Australia in certain circumstances.<sup>56</sup> As noted in Chapter 4, the provisions in the *Census and Statistics Act* are complemented by s 30A of the *Archives Act 1983* (Cth) which prohibits an Archives officer from disclosing census information before the information is available for public access.

5.53 The ABS produces statistics on a wide range of social and economic matters. Several provisions of the *Census and Statistics Act* deal with the disclosure of information given under the Act. Section 12 of the Act provides that the results of any analysis of statistical information shall not be published in a manner that is likely to enable the identification of a particular person or organisation, while s 13(3) provides that information about a person shall not be disclosed under s 13(1) in a manner that is likely to enable the identification of that person.

### ***Electoral information***

5.54 The *Commonwealth Electoral Act 1918* (Cth) requires the Australian Electoral Commission (AEC) to 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 AEC.<sup>57</sup> Only the names and addresses of enrolled voters are included on the publicly available electoral roll.

5.55 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’.<sup>58</sup> In addition, the *Commonwealth Electoral Act* allows for the disclosure of electoral information to a number of people and bodies, including Members of Parliament, political parties and approved medical researchers.<sup>59</sup> This information may only be used for certain purposes.<sup>60</sup>

5.56 The *Commonwealth Electoral Act* contains secrecy provisions aimed at protecting the unauthorised disclosure of electoral information. Section 90B prohibits the disclosure of certain information, such as information about defence and Australian Federal Police (AFP) personnel, to anyone.<sup>61</sup> Section 91B of the Act makes it an offence for a person to disclose information obtained under s 90B, unless the disclosure ‘would be a use of the information for a permitted purpose under s 91A’. Section 189B makes it an offence to disclose information obtained from an electronic list of postal

---

56 Ibid s 8A.

57 *Commonwealth Electoral Act 1918* (Cth) s 90A.

58 Australian Electoral Commission, *How to View the Commonwealth Electoral Roll* <[http://www.aec.gov.au/Enrolling\\_to\\_vote/About\\_Electoral\\_Roll/](http://www.aec.gov.au/Enrolling_to_vote/About_Electoral_Roll/)> at 6 November 2008.

59 *Commonwealth Electoral Act 1918* (Cth) s 90B.

60 Ibid s 91A. For further discussion of the privacy framework governing the use of the electoral roll see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [16.136]–[16.154].

61 *Commonwealth Electoral Act 1918* (Cth) s 90B (6), (7), (8A).

vote applicants provided by the AEC, if the disclosure ‘would not be a use of the information for a permitted purpose’. Finally, s 323 makes it an offence for an officer or scrutineer to disclose any information with respect to the vote of an elector that was acquired under the Act or regulations in a manner that is likely to enable the identification of the elector.

### **Defence or security information**

5.57 A little over 5% of Commonwealth secrecy provisions aim to prevent the unauthorised disclosure of defence or security information. Historically, the protection of this kind of information is a core function of secrecy provisions. Most secrecy provisions that protect defence or security information criminalise the unauthorised disclosure of this information. Disclosure can also attract criminal penalties under s 79 of the *Crimes Act* (disclosure of official secrets) and s 91.1 of the *Criminal Code* (Cth) (espionage).

5.58 Some provisions that protect defence or security information expressly prohibit the disclosure of certain information. For example, s 73A of the *Defence Act 1903* (Cth) makes it an offence for a member of the Australian Defence Force (ADF), or a person engaged or appointed under the *Public Service Act*, to communicate, otherwise than in the course of his or her official duty,

any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air force aerodrome or establishment or any other naval, military or air force information.

5.59 Other provisions prohibit the disclosure of any information if the disclosure ‘is likely to’ prejudice the security or defence of Australia.<sup>62</sup> Such provisions are a rare example of an express requirement that the disclosure be likely to cause some kind of harm. In some provisions, a designated person determines the threshold question of whether information will prejudice the security or defence of Australia. For example, s 108 of the *Designs Act 2003* (Cth) provides that the Registrar of Designs may prohibit or restrict the publication of information about the subject matter of a design application if it appears to be ‘necessary or expedient to do so in the interests of the defence of the Commonwealth’.<sup>63</sup>

5.60 Criminal offences relating to the disclosure of official secrets also fall within this category. Section 79 of the *Crimes Act* creates a number of offences relating to the use and disclosure of ‘prescribed information’, which is defined in s 79(1) and includes three kinds of information:

---

62 See, eg, *Defence Force Discipline Act 1982* (Cth) s 58(1).

63 See also *Auditor-General Act 1997* (Cth) s 37; *Patents Act 1990* (Cth) s 173; *Privacy Act 1988* (Cth) s 70; *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24.

- information made or obtained in contravention of pt VII of the *Crimes Act* (ie, by unlawful sounding) or s 91.1 of the *Criminal Code* (ie, by espionage);
- information relating to a prohibited place or anything in a prohibited place that the person knows, or ought to know by reason of the nature of the information or circumstances by which it came into a person's possession, should not be communicated;<sup>64</sup> or
- information made or obtained by a Commonwealth officer or a person holding office under the Queen owing to his or her position, which, by reason of the nature or circumstances under which the information was made or obtained, or for any other reason, it is his or her duty to treat as secret.

5.61 The first two categories relate to particular kinds of defence and security information. However, the third category is more general in application and is discussed further below in the context of the discussion of general criminal offences.

5.62 The offences created by s 79 of the *Crimes Act* extend beyond Commonwealth officers to cover the communication or receipt of prescribed information by any person. The most serious offence created by s 79 is the offence of communicating, retaining or receiving an official secret with the intention of prejudicing the security or defence of the Commonwealth. This provision, and s 91.1 of the *Criminal Code* discussed in the next paragraph, are notable among statutory secrecy provisions for explicitly referring to an intention to cause harm.<sup>65</sup> The maximum penalty for these offences is seven years imprisonment.<sup>66</sup> Where there is no intention to prejudice security or defence, the unauthorised communication or receipt of such information attracts a maximum penalty of two years imprisonment,<sup>67</sup> while unauthorised retention is punishable by a maximum penalty of 6 months imprisonment.<sup>68</sup>

5.63 Section 91.1 of the *Criminal Code*, which sets out the offence of espionage, also falls into this category. Section 91.1(1) makes it an offence for a person to communicate information concerning the security or defence of the Commonwealth or another country to a foreign country or organisation with the intention of prejudicing the security or defence of the Commonwealth, or of giving an advantage to another country's security or defence. It is also an offence to make, obtain or copy such information with the intention of delivering it to a foreign country or organisation in order to prejudice the security or defence of the Commonwealth<sup>69</sup> or give an advantage

---

<sup>64</sup> 'Prohibited place' is defined in *Crimes Act 1914* (Cth) s 80 and includes defence property and installations.

<sup>65</sup> Chapter 10 includes further discussion on a requirement of harm in secrecy offences.

<sup>66</sup> *Crimes Act 1914* (Cth) ss 79(2), 79(5).

<sup>67</sup> *Ibid* s 79(3), (6).

<sup>68</sup> *Ibid* s 79(4).

<sup>69</sup> *Criminal Code* (Cth) s 91.1(3).

to another country's security or defence.<sup>70</sup> All offences in s 91.1 carry a maximum penalty of 25 years imprisonment.

5.64 Espionage offences were previously located in pt VII of the *Crimes Act*. The offence was repealed and re-enacted (in different terms) in the *Criminal Code* as part of the reforms included in the *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth).

5.65 This Act also made amendments to s 79 of the *Crimes Act* to replace the phrase 'intention of prejudicing the *safety* or defence of the Commonwealth' with the phrase 'intention of prejudicing the *security* or defence of the Commonwealth'. The Explanatory Memorandum states:

The change to the term 'security or defence' in the Bill reflects the modern intelligence environment. The term 'security' is intended to capture information about the operations, capabilities and technologies, methods and sources of Australian intelligence and security agencies. The term 'safety' is unlikely to include such information.<sup>71</sup>

5.66 The term 'security or defence' is not defined in the *Crimes Act*. The *Criminal Code Amendment Act* also added s 90.1 to the *Criminal Code* to define 'security or defence of a country' for the purposes of pt 5.2 of the *Criminal Code* as including 'the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies'. The Explanatory Memorandum envisaged that this definition was to apply to s 79 of the *Crimes Act*,<sup>72</sup> and it is likely that the phrase in s 79 would be interpreted consistently with the *Criminal Code*.

### **Law enforcement and intelligence information**

5.67 About 5% of secrecy provisions aim to protect information about the operations or investigations of law enforcement and intelligence agencies by prohibiting the unauthorised disclosure of a wide range of law enforcement and intelligence information. Some prohibit the disclosure of information if its disclosure could prejudice the conduct of an investigation or inquiry.<sup>73</sup> Others identify specific types of protected information, such as information about the existence of a law enforcement operation or investigation;<sup>74</sup> the existence or content of a warrant;<sup>75</sup> the questioning or

---

70 Ibid s 91.1(4).

71 Revised Explanatory Memorandum, *Criminal Code Amendment (Espionage and Related Matters) Bill 2002* (Cth).

72 Ibid.

73 See, eg, *Australian Crime Commission Act 2002* (Cth) s 9(4); *Privacy Act 1988* (Cth) s 70; *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1).

74 *Australian Crime Commission Act 2002* (Cth) s 29B (1), (3).

75 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS; *Telecommunications (Interception and Access) Act 1979* (Cth) ss 63, 133.

detention of a person in connection with a warrant;<sup>76</sup> the identity of an intelligence officer;<sup>77</sup> and the identity of a participant in the National Witness Protection Program.<sup>78</sup>

5.68 Further, financial intelligence information collected under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) is protected from unauthorised disclosure,<sup>79</sup> as is information intercepted or accessed under the *Telecommunications (Interception and Access) Act 1979* (Cth)<sup>80</sup> or obtained under the *Surveillance Devices Act 2004* (Cth).<sup>81</sup> Some secrecy provisions also prohibit the unauthorised disclosure of information obtained when conducting a forensic procedure on a suspect, offender or volunteer.<sup>82</sup>

5.69 As noted above in relation to defence and security information, offences relating to official secrets and espionage may also cover the disclosure of intelligence information.

### ***Confidential information***

5.70 About 10% of secrecy provisions aim to prevent the unauthorised disclosure of confidential information. Some provisions prohibit the disclosure of ‘confidential’ information, which may or may not be defined in the Act.<sup>83</sup> Others prohibit the disclosure of information that was supplied in confidence,<sup>84</sup> or information the disclosure of which would constitute a breach of confidence.<sup>85</sup> The most general provision of this kind is reg 2.1(4) of the *Public Service Regulations*, which provides that:

An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee’s employment if the information:

- (a) was, or is to be, communicated in confidence within the government; or
- (b) was received in confidence by the government from a person or persons outside the government;

whether or not the disclosure would found an action for breach of confidence.

---

76     *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS.

77     *Intelligence Services Act 2001* (Cth) s 41; *Australian Security Intelligence Organisation Act 1979* (Cth) s 92.

78     *Witness Protection Act 1994* (Cth) s 22.

79     *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 121, 122, 123, 127, 128, 130, 131.

80     *Telecommunications (Interception and Access) Act 1979* (Cth) ss 63, 133.

81     *Surveillance Devices Act 2004* (Cth) s 45.

82     See, eg, *Crimes Act 1914* (Cth) s 23YO.

83     See, eg, *Water Act 2007* (Cth) s 215 (in which confidential information is not expressly defined); cf *Offshore Minerals Act 1994* (Cth) s 374 (in which ‘confidential information’ is defined in s 27).

84     See, eg, *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) ss 604-15, 604-20; *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32; *Therapeutic Goods Act 1989* (Cth) s 9C.

85     *Industry Research and Development Act 1986* (Cth) s 47(1).

5.71 In addition, approximately 10% of secrecy provisions protect confidential commercial information. Some of these provisions specify the type of confidential commercial information protected,<sup>86</sup> while others prohibit the disclosure of information obtained under an Act on the basis that its disclosure would be detrimental to the commercial interests of a person or body. For example, s 74 of the *Wheat Export Marketing Act 2008* (Cth) prohibits the disclosure of ‘protected confidential information’, which is defined as information provided under certain provisions of the Act, the disclosure of which could cause financial loss or detriment to a person or benefit a competitor of the person.<sup>87</sup>

### ***Indigenous sacred or sensitive information***

5.72 A small number of Commonwealth secrecy provisions prohibit the disclosure of information that is considered sacred or otherwise significant by Indigenous peoples. For example, s 193S(3)(b) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth) prohibits the disclosure by a designated person<sup>88</sup> of any information that he or she is aware is considered sacred or significant by a particular group of Aboriginal persons or Torres Strait Islanders, where its disclosure would be inconsistent with the views or sensitivities of the members of the group. Similarly, s 41 of the *Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989* (Cth) provides that the Institute must not disclose information if the disclosure would be inconsistent with the views or sensitivities of relevant Aboriginal persons or Torres Strait Islanders.<sup>89</sup>

### ***Other information***

5.73 The ALRC has also identified secrecy provisions that aim to protect other types of Commonwealth information, including information that:

- would disclose the deliberations of the Cabinet;<sup>90</sup>
- would disclose the deliberations or advice of the Executive Council;<sup>91</sup>
- would prejudice the international relations of the Commonwealth;<sup>92</sup>
- would prejudice relations between the Commonwealth and a state;<sup>93</sup>

<sup>86</sup> See, eg, *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s 162.

<sup>87</sup> *Wheat Export Marketing Act 2008* (Cth) s 73. See also *Auditor-General Act 1997* (Cth) s 37.

<sup>88</sup> As defined in 193S(1) of the Act.

<sup>89</sup> See also *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3)(d).

<sup>90</sup> *Auditor-General Act 1997* (Cth) s 37(1), (2)(b); *Privacy Act 1988* (Cth) s 70(1)(c); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(c).

<sup>91</sup> *Privacy Act 1988* (Cth) s 70(1)(d); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(d).

<sup>92</sup> *Auditor-General Act 1997* (Cth) s 37(1), (2)(a); *Privacy Act 1988* (Cth) s 70(1)(a); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(a).

<sup>93</sup> *Auditor-General Act 1997* (Cth) s 37(1), (2)(c); *Privacy Act 1988* (Cth) s 70(1)(b); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(b).

- could form the basis for a claim by the Crown in right of the Commonwealth in a judicial proceeding that the information should not be disclosed;<sup>94</sup>
- is derived from, or related to, a complaint;<sup>95</sup>
- would endanger the safety of any person;<sup>96</sup>
- relates to an alternative dispute resolution process;<sup>97</sup>
- is derived from inspecting records;<sup>98</sup>
- would reveal that a person was acting in a certain capacity;<sup>99</sup> or
- relates to an investigation conducted by a safety compliance agency.<sup>100</sup>

### **Whose activity is regulated?**

5.74 The ALRC's mapping exercise shows that there is considerable variation in the way that the persons regulated by Commonwealth secrecy laws are described. Secrecy provisions are stated variously to apply to:

- Commonwealth agencies;
- Commonwealth officers and former officers;
- organisations or individuals providing services for or on behalf of the Commonwealth;
- other specific categories of organisation or individual; and/or
- any person.

---

94 *Auditor-General Act 1997* (Cth) s 37(1), (2)(f).

95 *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63(2); *Sex Discrimination Act 1984* (Cth) s 92(1).

96 *Australian Crime Commission Act 2002* (Cth) s 9(4); *Privacy Act 1988* (Cth) s 70(1)(h); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(h).

97 *Workplace Relations Act 1996* (Cth) ss 702, 707, 712, 715, sch 6 cl 38(5).

98 *Ibid* sch 1, cl 276; *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) s 183-1; *Copyright Act 1968* (Cth) s 203E(10).

99 *Workplace Relations Act 1996* (Cth) ss 165, 425, 485, 486, 668(3)(f).

100 *Transport Safety Investigation Act 2003* (Cth) ss 53, 60; *Space Activities Act 1998* (Cth) s 96; *Civil Aviation Act 1988* (Cth) s 32AP.

### **Commonwealth agencies**

5.75 Some secrecy provisions apply to agencies or statutory corporations, as distinct from individuals.<sup>101</sup> In 1990, John McGinness noted the growth in statutory authorities with power to require the production of information and the related growth in secrecy provisions applying to those authorities.<sup>102</sup> Such provisions are often expressed to bind the head and staff of an agency or other officers of the statutory authority.<sup>103</sup> Bodies corporate, as well as individuals, may be found guilty of a criminal offence.<sup>104</sup>

### **Commonwealth officers**

5.76 Approximately one third of all Commonwealth secrecy provisions apply to Commonwealth officers. In some cases, the provisions regulate specific agency heads or officers,<sup>105</sup> or all officers of specific Commonwealth agencies.<sup>106</sup> In other cases the provisions apply to all Commonwealth officers,<sup>107</sup> or all employees of the APS.<sup>108</sup>

5.77 Regulation 2.1 of the *Public Service Regulations* sets out the general duty of an APS employee not to disclose official information. An APS employee is defined in s 7 of the *Public Service Act* to mean a person engaged by an agency head for the purposes of the agency or as an APS employee by the Public Service Commissioner in a specified agency as the result of an administrative rearrangement. An agency is defined to mean a department, an executive agency established by the Governor-General, or a statutory agency.<sup>109</sup>

5.78 Section 70 of the *Crimes Act* regulates conduct by ‘Commonwealth officers’. The definition of the term ‘Commonwealth officer’ in s 70 is discussed in further detail below, but includes APS, ADF and AFP employees.<sup>110</sup>

### **Service providers to the Commonwealth**

5.79 Some secrecy provisions expressly refer to a wider range of individuals than is encompassed by the definition of Commonwealth officer, reflecting changes to the structure of government and government service provision, and the view that

101 For example, *Australian Securities and Investments Commission Act 2001* (Cth) s 127(1) applies to the Australian Securities and Investments Commission; and *Trade Practices Act 1974* (Cth) s 95ZP applies to the Australian Competition and Consumer Commission.

102 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 49.

103 See, eg, *Inspector-General of Taxation Act 2003* (Cth) s 37; *Australian Crime Commission Act 2002* (Cth) s 51; *Ombudsman Act 1976* (Cth) s 35.

104 *Criminal Code* (Cth) pt 2.5.

105 For example, *Ombudsman Act 1976* (Cth) s 35C applies to the Commonwealth Ombudsman.

106 For example, *Australian Postal Corporation Act 1989* (Cth) ss 90H, 90LB apply to ‘employees of Australia Post’ by virtue of s 90G.

107 For example, *Income Tax Assessment Act 1936* (Cth) s 16.

108 *Public Service Regulations 1999* (Cth) reg 2.1.

109 *Public Service Act 1999* (Cth) s 7.

110 *Crimes Act 1914* (Cth) s 3.

information should be protected at every point in the ‘distribution chain’, including where that information is handled outside the public sector.<sup>111</sup>

5.80 Around 10% of current secrecy provisions expressly regulate consultants<sup>112</sup> and others who provide goods or services for or on behalf of the Australian Government.<sup>113</sup> In addition, service providers are often required by agencies to comply with confidentiality undertakings as part of service provision arrangements.<sup>114</sup>

#### ***Other organisations and individuals***

5.81 Specific secrecy provisions regulate a wide range of other organisations and individuals. For example, secrecy provisions may regulate:

- state, territory or local government employees;<sup>115</sup>
- organisations and individuals who engage in federally funded or regulated areas of the private sector—for example, aged care providers;<sup>116</sup> and
- individuals assisting in government studies or inquiries;<sup>117</sup>

#### ***Any person***

5.82 A number of secrecy provisions, in particular those relating to defence and national security, regulate the activities of *any* person who comes into possession or control of documents or information.<sup>118</sup> Section 79 of the *Crimes Act*, for example, prohibits unauthorised handling or communication of official secrets by any person, which would include, for example, members of the media.

5.83 Around 30% of Commonwealth secrecy provisions are stated to apply to the handling of information by ‘any person’. However, other language used in these secrecy provisions, and the practical context in which the provisions operate, mean that the provisions will apply mainly to Commonwealth officers or contracted service providers. For example, the information protected by the provision may be defined as information ‘acquired by the person in the course of performing duties or exercising

111 Australian Parliament—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), [7.11.2].

112 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32(1).

113 See, eg, *Customs Administration Act 1985* (Cth) s 16.

114 Confidentiality clauses are included in contracts with service providers as a matter of course: Australian Parliament—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), 53.

115 See, eg, *Taxation Administration Act 1953* (Cth) s 13J.

116 See, eg, *Aged Care Act 1997* (Cth) s 62-1.

117 See, eg, *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 4; *Inspector of Transport Security Act 2006* (Cth) s 35(7).

118 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9(2).

powers or functions' under certain legislation;<sup>119</sup> or as information obtained for the purposes of certain legislation and held in the records of specific agencies.<sup>120</sup>

#### **Current and former parties**

5.84 About 25% of secrecy provisions expressly regulate the behaviour of persons who have access to Commonwealth information because of their current position, as well as those who have had access in the past but may no longer have access. For example, s 70 of the *Crimes Act* regulates the behaviour of both current and former Commonwealth officers.

5.85 An example of a specific secrecy provision governing both current and former officers is s 191 of the *Aboriginal and Torres Strait Islander Act 2005* (Cth), which expressly applies to a person:

- (a) who is or has been an Indigenous Business Australia Director or acting Indigenous Business Australia Director;
- (b) who is or has been the Indigenous Business Australia General Manager or an acting Indigenous Business Australia General Manager;
- (c) who is or has been employed or engaged under section 175 or 178;
- (d) who is performing, or who has performed, duties on behalf of Indigenous Business Australia pursuant to an arrangement under section 176; or
- (e) whose services are being or have been made available to Indigenous Business Australia pursuant to an arrangement under section 177.

5.86 The application of s 70 of the *Crimes Act* may also extend the application of statutory secrecy offences to former Commonwealth officers. For example, as noted in Chapter 4 and referred to above, s 30A(1) of the *Archives Act 1983* (Cth) provides that:

An Archives officer must not, at any time before a record containing Census information from a Census is in the open access period for that Census, divulge or communicate any of that information to another person (except to another Archives officer for the purposes of, or in connection with, the performance of that other officer's duties under this Act).

5.87 Although this section does not expressly refer to both current and former Archives officers, a note to s 30A(1) draws attention to the criminal offence created by s 70 of the *Crimes Act* in relation to the disclosure of information by those who are, or have been, Commonwealth officers. Section 30A of the *Archives Act* imposes a duty on current Archives officers who are engaged under the *Public Service Act*<sup>121</sup> and therefore fall within the definition of 'Commonwealth officer' in s 3 of the *Crimes Act*. The effect of s 70 is to create an offence for both current and former Archives officers who publish or communicate 'any fact of document which comes to his or her

---

119 For example, *Aged Care Act 1997* (Cth) s 86-2.

120 For example, *Student Assistance Act 1973* (Cth) ss 353, 3(1) definition of 'protected information'.

121 *Archives Act 1983* (Cth) s 9.

knowledge, or into his or her possession, by virtue of being a Commonwealth officer, and which it is his or her duty not to disclose’—in this case, census information that is not in the open access period—without lawful authority or excuse.

### **What kind of activity is regulated?**

5.88 The third aspect of secrecy provisions is the regulation of particular conduct or activities in relation to the information. The vast majority (90%) of secrecy provisions prohibit disclosing, divulging or communicating Commonwealth information. In addition, conduct such as tabling information in Parliament, or serving information on other parties, can be regarded as regulated forms of disclosure.

5.89 Secrecy provisions may also regulate other activities such as making a record (approximately 30% of secrecy provisions), using information (approximately 20%) or soliciting information (less than 5%).

5.90 A small number of provisions focus on obtaining information. For example, under s 203 of the *Social Security (Administration) Act 1999* (Cth), a person commits an offence if he or she intentionally obtains information without authorisation and knew or ought reasonably to have known that the information was protected information.<sup>122</sup>

5.91 The ALRC’s mapping exercise has identified very few provisions that regulate the possession or receipt of information. One example is s 79(5) of the *Crimes Act*:

If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing or having reasonable ground to believe, at the time when he or she receives it, that it is communicated to him or her in contravention of section 91.1 of the *Criminal Code* or subsection (2) of this section, he or she shall be guilty of an indictable offence unless he or she proves that the communication was contrary to his or her desire.<sup>123</sup>

### **Initial and subsequent disclosures**

5.92 Some secrecy provisions regulate both the initial and any subsequent unauthorised handling of Commonwealth information. For example, under s 23E of the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth):

- (4) A person commits an offence if:
  - (a) information is communicated to the person (the *first person*) in accordance with [the Act]; and
  - (b) the information is communicated by a person (the *second person*) to whom this section applies; and

---

122 See also *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 163; *Student Assistance Act 1973* (Cth) s 352; *Child Care Act 1972* (Cth) s 12K; *Defence Act 1903* (Cth) s 73A(2).

123 *Crimes Act 1914* (Cth) s 79(6) creates a similar offence in relation to material that is in contravention of s 79(3) of the *Crimes Act*.

- (c) the second person acquired the information because of his or her membership of, or employment by, a Land Council or his or her activities as an authorised person; and
- (d) the information concerns the affairs of a third person; and
- (e) the first person, either directly or indirectly, makes a record of, or divulges or communicates the information to any other person.

5.93 Some provisions make it an offence for a recipient of certain information to then use or disclose that information for other purposes. For example, under s 86–3 of the *Aged Care Act 1997* (Cth), the Secretary of the Department of Health and Ageing may disclose protected information in certain circumstances, including to other government departments, such as Centrelink or Medicare, or where there is a risk to health and safety. Under s 86–5, it is an offence for a person who receives information by virtue of s 86–3 to make a record of, disclose or otherwise use the information other than for the purpose for which the information was disclosed.

5.94 However, the vast majority of secrecy provisions mapped by the ALRC do not contain a prohibition on disclosure by third party recipients.

### **Method of regulation**

5.95 The fourth aspect of secrecy provisions is the way in which the disclosure of information is regulated. Around 70% of secrecy provisions establish criminal offences and around 75% of these are indictable offences—that is, offences punishable by imprisonment for a period exceeding 12 months.<sup>124</sup> The remainder are summary offences—that is, offences which are not punishable by imprisonment, or are punishable by imprisonment for a period not exceeding 12 months.<sup>125</sup> The ALRC has identified only three civil penalty provisions.<sup>126</sup>

5.96 The ALRC’s mapping exercise indicates that the great majority of Commonwealth secrecy offences do not stipulate fault elements. In these circumstances, the *Criminal Code* sets out the fault elements that apply, so that

- for a physical element consisting of conduct, the fault element is intention;<sup>127</sup> and
- for a physical element consisting of a circumstance or a result, the fault element is recklessness.<sup>128</sup>

---

124 Ibid s 4G.

125 Ibid s 4H.

126 *Workplace Relations Act 1996* (Cth) s 715, sch 1 s 276; *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 170B. Civil penalty provisions are discussed in Ch 6.

127 *Criminal Code* (Cth) s 5.6(1).

128 Ibid s 5.6(2).

5.97 By way of example, s 19 of the *Census and Statistics Act 1905* (Cth) provides that:

A person commits an offence if:

- (a) the person is, or has been, the Statistician or an officer; and
- (b) the person, either directly or indirectly, divulges or communicates to another person (other than the person from whom the information was obtained) any information given under this Act.

Penalty: 120 penalty units or imprisonment for 2 years, or both.

5.98 Applying the rules set out in the *Criminal Code*, the relevant physical and fault elements for this offence can be set out as follows:

<b>Physical element</b>	<b>Fault element</b>
Conduct = directly or indirectly divulges or communicates information to another person	intention
Circumstance = the information was given under the Act	recklessness

5.99 Around 30% of the secrecy provisions identified by the ALRC do not expressly criminalise the wrongful handling of Commonwealth information but rather establish rules for the handling of this information. As noted above, while such provisions are not, in themselves, offences, s 70 of the *Crimes Act* may operate to attach criminal sanctions to the breach of these rules by a Commonwealth officer.

### Exceptions and defences

5.100 The final feature of many secrecy provisions involves exceptions or defences. An ‘exception’ is a provision that limits the scope of conduct prohibited by a secrecy law, while a ‘defence’ is a provision that may excuse conduct that is otherwise prohibited by a secrecy provision. An exception or defence may provide, for example, that a Commonwealth officer does not commit an offence, or has a defence, where disclosure of information is made in the course of performing duties under the relevant legislation. Exceptions are more commonly included in Commonwealth secrecy laws than defences.

5.101 About 15% of secrecy provisions do not contain any express exceptions or defences.<sup>129</sup> However, defences may nevertheless be available under provisions of the *Criminal Code* or at common law. In particular, the *Criminal Code* sets out general principles of criminal responsibility applicable to offences against the laws of the Commonwealth. The Code provides, for example, that even if an offence provision is

---

129 See, eg, *Crimes Act 1914* (Cth) s 70.

stated to be an offence of strict liability, the defence of mistake of fact remains available.<sup>130</sup>

5.102 Express exceptions or defences are included in most Commonwealth secrecy provisions. The following discussion summarises exceptions and defences currently contained in secrecy laws within a number of broad categories.

#### ***Performance of functions and duties***

5.103 Approximately 35% of secrecy provisions allow information handling in the performance of a person's functions and duties as an employee or officer. Taxation secrecy laws, for example, generally allow information handling in the 'course of duties of an officer'. Secrecy obligations placed on officers by the *Taxation Administration Act 1953* (Cth) do not apply 'to the extent that the person makes a record of the information, or divulges or communicates the information ... in the performance of the person's duties as an officer'.<sup>131</sup> Similar formulations appear in other areas of Commonwealth legislation.<sup>132</sup>

#### ***Required or authorised by law***

5.104 Many secrecy provisions incorporate exceptions that allow the handling of information as required or authorised by law.<sup>133</sup> Secrecy provisions commonly provide that information may be handled 'for the purposes of this Act'.<sup>134</sup> It is also common for secrecy provisions to permit disclosure for the purposes of other legislation,<sup>135</sup> or intergovernmental arrangements.<sup>136</sup>

#### ***Authorisation by specified persons***

5.105 About 15% of secrecy provisions permit the disclosure of information at the discretion of specified office-holders or other persons. For example, the *Superannuation Industry (Supervision) Act 1993* (Cth) provides that it is not an offence to disclose information where disclosure is 'approved by the Commissioner of Taxation by instrument in writing'.<sup>137</sup>

---

130 See *Criminal Code* (Cth) ss 6.1, 9.2.

131 *Taxation Administration Act 1953* (Cth) s 3C(2A).

132 *Racial Discrimination Act 1975* (Cth) s 27F(3A); *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2); *Disability Services Act 1986* (Cth) s 28(2A).

133 There is an extensive discussion of the meaning of the phrase 'required or authorised by or under law' in the context of the *Privacy Act 1988* (Cth) in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Ch 16.

134 See eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 65(4); *Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992* (Cth) s 14(3A); *Taxation Administration Act 1953* (Cth) s 3C(2A).

135 See, eg, *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 49(3); *Reserve Bank Act 1959* (Cth) s 79A(2).

136 See, eg, *Disability Discrimination Act 1992* (Cth) s 127(3).

137 *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C(5)(b).

5.106 Other secrecy provisions permit information handling to be authorised by specified persons—generally the head of an agency or the responsible minister—provided that other criteria are met. For example:

- the *Customs Administration Act 1985* (Cth) provides an exception to secrecy provisions where the disclosure of information is authorised by the Chief Executive Officer of Customs and the information will be used by another Australian Government agency for the purposes of that agency's functions;<sup>138</sup>
- the *Health Insurance Act 1973* (Cth) provides an exception to secrecy provisions where the Minister certifies, by instrument in writing, that it is necessary in the public interest that information be disclosed;<sup>139</sup> and
- the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) provides an exception to secrecy provisions where access to information is for the purposes of investigating a breach of a law of the Commonwealth and is authorised by the Chief Executive Officer of the Australian Transaction Reports and Analysis Centre.<sup>140</sup>

#### ***Disclosure to specified persons or entities***

5.107 Approximately 30% of secrecy provisions provide exceptions where disclosure is made to specified persons or entities such as ministers or government (Australian, state or territory) agencies or officials. For example:

- the *Australian Prudential Regulation Authority Act 1998* (Cth) provides exceptions to secrecy provisions where disclosure of information is to the Australian Statistician, the Reserve Bank of Australia, auditors and actuaries;<sup>141</sup>
- the *Industry Research and Development Act 1986* (Cth) provides that secrecy provisions do not apply to the disclosure of information to the Minister, ministerial staff, the Secretary of the Department or a designated officer of the Department;<sup>142</sup> and
- the *Gene Technology Act 2000* (Cth) provides exceptions to secrecy provisions where disclosure is made in the course of carrying out duties or functions under the Act and is to ‘the Commonwealth or a Commonwealth authority’, a state agency, or the Gene Technology Technical Advisory Committee.<sup>143</sup>

---

138 *Customs Administration Act 1985* (Cth) s 16(3).

139 *Health Insurance Act 1973* (Cth) s 130(3).

140 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 129(1).

141 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(5A), (5B), (6A).

142 *Industry Research and Development Act 1986* (Cth) s 47(2).

143 *Gene Technology Act 2000* (Cth) s 187(1)(d).

5.108 A particular focus of such exceptions is to authorise information sharing among Australian Government agencies. The *Australian Prudential Regulation Authority Act*, the *Customs Administration Act*, and the *Income Tax Assessment Act 1936* (Cth), for example, each contains provisions authorising the disclosure of certain information to the ABS.<sup>144</sup>

5.109 In some instances, secrecy provisions permit disclosure in circumstances, or to persons or entities, as prescribed by regulation. For example, the *Medical Indemnity Act 2002* (Cth) allows disclosure of information to a prescribed authority or person.<sup>145</sup> The *Building and Construction Industry Improvement Act 2005* (Cth) provides an exception where disclosure is in accordance with regulations.<sup>146</sup>

### ***Legal proceedings***

5.110 About 15% of secrecy provisions provide exceptions to expressly permit the handling of information for the purposes of court or tribunal proceedings.<sup>147</sup>

5.111 However, secrecy provisions more often provide that government office-holders, employees or other persons are not required to disclose information in court or tribunal processes, other than for the purposes of the particular enactment.<sup>148</sup> As noted in Chapter 1, the extent to which Commonwealth officers can be compelled to provide information in the course of investigations or in legal proceedings is not a focus of this Inquiry.

### ***Law enforcement purposes***

5.112 Approximately 15% of secrecy provisions provide exceptions to allow the handling of information for various law enforcement and investigatory purposes. These provisions often refer to the investigation of criminal offences.<sup>149</sup>

5.113 Exceptions may extend beyond the investigation of criminal offences to broader law enforcement and administration of justice concerns. For example:

---

144 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(5A); *Customs Administration Act 1985* (Cth) s 16(9)(ea); *Income Tax Assessment Act 1936* (Cth) s 16(4)(ga). See further Ch 3 on sharing Commonwealth information.

145 *Medical Indemnity Act 2002* (Cth) s 77(4).

146 *Building and Construction Industry Improvement Act 2005* (Cth) s 65(4).

147 See, eg, *Surveillance Devices Act 2004* (Cth) s 45(5); *Pooled Development Funds Act 1992* (Cth) s 71(2); *Fringe Benefits Tax Assessment Act 1986* (Cth) s 5(5).

148 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32(2); *Child Support (Assessment) Act 1989* (Cth) s 150(5); *Australian Security Intelligence Organisation Act 1979* (Cth) s 81(2).

149 See, eg, *Surveillance Devices Act 2004* (Cth) s 45(5); *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(a); *Crimes Act 1914* (Cth) s 23YO(2), relating to the disclosure of forensic DNA information.

- the *Crimes Act* allows forensic DNA information to be disclosed for the purposes of a coronial inquest or inquiry, or an investigation by the Privacy Commissioner or Ombudsman;<sup>150</sup>
- the *Child Support (Assessment) Act 1989* (Cth) allows the communication of information about missing and deceased persons where necessary to assist a court, coronial inquiry, Royal Commission, or department or authority of the Commonwealth, a state or a territory;<sup>151</sup> and
- the *Australian Federal Police Act 1979* (Cth) allows the Commissioner to approve the disclosure of information that relates to the National Witness Protection Program if he or she is of the opinion that it is ‘in the interests of the due administration of justice to do so’.<sup>152</sup>

### ***Consent***

5.114 About 20% of secrecy provisions provide exceptions that permit the disclosure of information where the person or entity to whom the information relates has consented to the disclosure.<sup>153</sup>

5.115 In some instances, where legislation provides exceptions permitting the handling of information, these are subject to further exceptions in relation to the disclosure of personal information, as that term is defined in the *Privacy Act*.<sup>154</sup> For example, under the *Customs Administration Act 1985* (Cth) certain authorised disclosures of personal information may take place only where the person to whom the information relates has consented.<sup>155</sup>

5.116 Some secrecy provisions permit disclosure of information after notice and an opportunity to object to disclosure has been provided to certain persons. For example, the *Food Standards Australia New Zealand Act 1991* (Cth) provides that confidential commercial information given by a person may not be disclosed unless the Chief Executive Officer of Food Standards Australia New Zealand has advised the person of this in writing and ‘given the person a reasonable opportunity to communicate the person’s views about the proposed disclosure of that information’.<sup>156</sup>

---

150     *Crimes Act 1914* (Cth) s 23YO(2).

151     *Child Support (Assessment) Act 1989* (Cth) s 150(4D)–(4F).

152     *Australian Federal Police Act 1979* (Cth) s 60A(2B).

153     See, eg, *Gene Technology Act 2000* (Cth) s 187(1)(f); *National Health Act 1953* (Cth) s 135A(8); *Reserve Bank Act 1959* (Cth) s 79A(3).

154     *Privacy Act 1988* (Cth) s 6(1). That is, information ‘about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion’.

155     *Customs Administration Act 1985* (Cth) s 16(7).

156     *Food Standards Australia New Zealand Act 1991* (Cth) s 114(5).

### ***De-identified information***

5.117 Less than 5% of secrecy provisions provide exceptions permitting the disclosure of information if it does not identify the person or entity that is the subject of the information.<sup>157</sup> For example:

- the *Australian Prudential Regulation Authority Act 1998* (Cth) states that it is not an offence if the information disclosed is ‘in the form of a summary or collection of information that is prepared so that information relating to any particular person cannot be found out from it’;<sup>158</sup>
- the *Census and Statistics Act 1905* (Cth) provides that certain information shall not be ‘published or disseminated in a manner that is likely to enable the identification of a particular person or organisation’;<sup>159</sup> and
- the *Epidemiological Studies (Confidentiality) Act 1981* (Cth) provides that the Act does not prohibit the publication of certain information from prescribed studies ‘but such conclusions, statistics or particulars shall not be published in a manner that enables the identification of an individual person’.<sup>160</sup>

### ***Disclosure to avert threats to life or health***

5.118 Some secrecy provisions contain exceptions permitting the disclosure of information in order to avert threats to a person’s life or health. Such exceptions are expressed in different ways, and may cover threats to a person’s life, health, safety or welfare. For example:

- the *Customs Administration Act 1985* (Cth) allows the disclosure of information necessary to ‘avert or reduce’ a ‘serious and imminent threat to the health or life of a person’;<sup>161</sup>
- the *Inspector-General of Intelligence and Security Act 1986* (Cth) allows the disclosure of information ‘necessary for the purpose of preserving the well-being or safety of another person’;<sup>162</sup> and
- the *Child Support (Assessment) Act 1989* (Cth) allows the disclosure of information to prevent or lessen a ‘credible threat to the life, health or welfare of a person’.<sup>163</sup>

---

157 The privacy implications of the use of de-identified information is discussed in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [6.64]–[6.87].

158 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(7).

159 *Census and Statistics Act 1905* (Cth) s 12(2).

160 *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 11.

161 *Customs Administration Act 1985* (Cth) s 16(3F).

162 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34(1A).

163 *Child Support (Assessment) Act 1989* (Cth) s 150(3)(e).

***Public interest***

5.119 A small number of secrecy provisions allow the disclosure of Commonwealth information when disclosure is in the public or national interest.

5.120 For example, the *Food Standards Australia New Zealand Act 1991* (Cth) allows the disclosure of certain information if the Minister certifies, by instrument, that it is necessary ‘in the public interest’.<sup>164</sup> Similar provisions are found in other statutes, including the *Medical Indemnity Act 2002* (Cth), *Health Insurance Act 1973* (Cth) and *National Health Act 1953* (Cth).<sup>165</sup>

5.121 In addition, the *Australian Security Intelligence Organisation Act 1979* (Cth) allows the disclosure of information where the information concerns matters outside Australia and the Director-General ‘is satisfied that the national interest requires the communication’.<sup>166</sup>

***Requirement of harm***

5.122 Some secrecy laws prohibit the disclosure of information only where the disclosure is likely to cause harm. For example, as noted above, reg 2.1 of the *Public Service Regulations 1999* (Cth) provides that an APS employee must not disclose information ‘if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs’.

5.123 A more specific example is the *Defence Force Discipline Act 1982* (Cth) which provides a defence to the offence of unauthorised disclosure of information where ‘the person proves that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to be prejudicial to the security or defence of Australia’.<sup>167</sup> Further examples of secrecy provisions that contain a requirement of harm are set out in Chapter 10.

## **General criminal offences**

5.124 The preceding section of this chapter has described key aspects of the numerous statutory secrecy provisions in Commonwealth legislation. Chapters 9, 10 and 11 review specific statutory offences and suggest how such offences could be simplified and framed in a consistent manner.

5.125 This section of the chapter examines the two general criminal offences in the *Crimes Act* relating to the unauthorised disclosure of Commonwealth information.

164 *Food Standards Australia New Zealand Act 1991* (Cth) s 114(4).

165 *Medical Indemnity Act 2002* (Cth) s 77(3); *Health Insurance Act 1973* (Cth) s 130(3); *National Health Act 1953* (Cth) s 135A(3).

166 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(b).

167 *Defence Force Discipline Act 1982* (Cth) s 58(3).

Section 70 covers the disclosure of information by Commonwealth officers, while s 79 deals with the disclosure of ‘official secrets’. The following overview analyses these sections according to criteria similar to that used to analyse the statutory secrecy provisions discussed above, that is:

- the type of information protected;
- the kinds of activities regulated;
- whose activity is regulated; and
- exceptions and defences.

### Section 70—disclosure of information by Commonwealth officers

5.126 Section 70 of the *Crimes Act* is the only provision remaining in pt VI of the *Crimes Act*.<sup>168</sup> A version of s 70 was included in the original *Crimes Act* in 1914, and was based on a provision of the *Criminal Code Act 1899* (Qld).<sup>169</sup> This original version of s 70 was repealed and replaced in 1960 to extend the prohibition on the unauthorised disclosure of information by Commonwealth officers to include *former* Commonwealth officers.<sup>170</sup> While minor amendments have been made to s 70 on three occasions since 1960,<sup>171</sup> the substance of the provision has not changed since that time.

5.127 Section 70 is set out in Chapter 1 and in Appendix 5. As it is the pivotal section in this Inquiry, it is instructive to repeat it here in full:

- (1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he or she is authorized to publish or communicate it, any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer, and which it is his or her duty not to disclose, shall be guilty of an offence.
- (2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him or her), any fact or document which came to his or her knowledge, or into his or her possession, by virtue of having been a Commonwealth officer, and which, at the time when he or she ceased to be a Commonwealth officer, it was his or her duty not to disclose, shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

<sup>168</sup> The other offence provisions in pt VI of the *Crimes Act 1914* (Cth) were repealed by the *Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Act 2000* (Cth) and replaced by more modern offence provisions in the *Criminal Code* (Cth).

<sup>169</sup> Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney-General), 265, 269; J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 53.

<sup>170</sup> *Crimes Act 1960* (Cth).

<sup>171</sup> *Crimes Amendment Act 1982* (Cth); *Statute Law (Miscellaneous Provisions) Act 1987* (Cth); *Statute Law Revision Act 2008* (Cth).

5.128 Section 70 does not specify the fault element for the offence. As noted above, in this situation the *Criminal Code* provides that the fault element for a physical element consisting of conduct is intention,<sup>172</sup> while for a physical element consisting of a circumstance or result, the fault element is recklessness.<sup>173</sup> Applying these rules, the relevant physical and fault elements of the offence in s 70 can be set out as follows:<sup>174</sup>

<b>Physical element</b>	<b>Fault element</b>
Conduct = publishes or communicates a fact or document	intention
Circumstance = the fact or document came into his or her possession by virtue of being a Commonwealth officer	recklessness
Circumstance = he or she had a duty not to disclose the fact or document	recklessness

5.129 There have been several successful prosecutions for breaches of s 70, including of:

- a member of the AFP for disclosing information held in AFP files to a private business associate;<sup>175</sup>
- an officer of the ATO for providing documents containing summaries of taxpayers and tax agents to a private business associate;<sup>176</sup>
- an officer of the Australian Customs Service for providing reports about security at Sydney Kingsford Smith Airport to journalists;<sup>177</sup>
- an officer of the Office of Indigenous Policy Coordination for disclosing information relating to the then draft *Declaration on the Rights of Indigenous Peoples* to her daughter, and information relating to Commonwealth Indigenous policy to a member of the Mutitjulu community in the Northern Territory;<sup>178</sup> and

<sup>172</sup> *Criminal Code* (Cth) s 5.6(1).

<sup>173</sup> Ibid s 5.6(2). Recklessness is defined in *Criminal Code* (Cth) s 5.4.

<sup>174</sup> The table is based on the elements of the offence in s 70(2) of the *Crimes Act* as summarised by Bell JA in *Kessing v The Queen* [2008] NSWCCA 310, [24].

<sup>175</sup> *Johnston v Director of Public Prosecutions* (Cth) (1989) 90 ACTR 7.

<sup>176</sup> *R v Petroulias (No 36)* [2008] NSWSC 626.

<sup>177</sup> *R v Kessing* [2007] NSWDC 138; *Kessing v The Queen* [2008] NSWCCA 310.

<sup>178</sup> *R v Goreng Goreng* [2008] ACTSC 74.

- an officer of Centrelink for disclosing personal details of Centrelink customers to a firm which offered to pay for information leading to the whereabouts of various people.<sup>179</sup>

5.130 The effect of s 70 is to apply criminal sanctions to the breach of secrecy obligations by public officials.<sup>180</sup> The following sections of this chapter examine elements of the provision in more detail.

**'Duty not to disclose'**

5.131 Section 70 does not create a duty to keep information secret or confidential. Rather, the source of such a duty must be found elsewhere. Most commonly, the source of the duty is a specific legislative provision giving rise to a duty not to disclose official information. For example, reg 2.1(3) of the *Public Service Regulations* provides that APS employees must not disclose information obtained or generated in connection with their employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government. This provision sets out a 'duty not to disclose' and, as such, can be used as the basis for a prosecution under s 70 of the *Crimes Act*.<sup>181</sup>

5.132 Other sources of the duty may be those considered earlier in this chapter—such as an employee's common law duty to serve his or her employer in good faith and fidelity or an equitable duty to protect his or her employer's confidential information. In addition, the terms and conditions of an employment contract, or the obligation imposed by s 13(10) of the *Public Service Act* not to use information for personal benefit, may establish a 'duty not to disclose'.

5.133 Leo Tsaknis has argued that in order for criminal sanctions to attach to the breach of a duty not to disclose, that duty must be a legal duty as opposed to a moral obligation or contractual arrangement.<sup>182</sup> However, in *Director of Public Prosecutions v G*, the Full Court of the Federal Court noted that a contractual obligation may be sufficient to constitute a duty for the purposes of the former s 72 of the *Crimes Act*, which provided for the offence of falsifying books or records by a Commonwealth officer 'fraudulently and in breach of his [or her] duty'.<sup>183</sup> However, the Court was not required to finally determine this issue.

5.134 Under s 70, criminal sanctions attach to a breach of a 'duty not to disclose'. This can be compared with s 79 of the *Crimes Act* (discussed below), which refers to a 'duty

179 Transcript of Proceedings, *R v Sweeney*, (District Court Queensland, Shanahan J, 28 March 2001).

180 P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 214.

181 See, eg. *R v Goreng Goreng* [2008] ACTSC 74, [8]; *Johnston v Director of Public Prosecutions (Cth)* (1989) 90 ACTR 7, 9–10.

182 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 259.

183 *Director of Public Prosecutions v G* (1999) 85 FCR 566, [78] referring to *Austin v Parsons* (1986) 40 SASR 534 and *R v Cushion* (1997) 141 FLR 392.

to treat [information] as secret'. The Western Australian Court of Criminal Appeal has held that the phrase 'duty not to disclose' is synonymous with the duty to 'keep secret' within the meaning of s 81 of the *Crimes Act 1913* (WA).<sup>184</sup> However, it may be that, for the purposes of Commonwealth law, the duty not to disclose is wider than the duty to keep information secret, in that secrecy presupposes that the material is not already in the public domain, while a duty not to disclose could apply to any information.<sup>185</sup>

### ***What kind of information is protected?***

5.135 Section 70 makes it an offence for a Commonwealth officer to disclose 'any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer'. On its face, s 70 could apply to the disclosure of any information regardless of its nature or sensitivity.

5.136 In *Commissioner of Taxation v Swiss Aluminium Australia Ltd*, Bowen CJ of the Federal Court commented that:

From the policy point of view it may be noted that an enactment such as s 70 of the *Crimes Act* prohibiting the disclosure of information obtained in the course of the duties of a public servant treats the nature or kind of information disclosed as virtually irrelevant. It is the office occupied by the person and the character in which he obtained the information which imposes the obligation of secrecy upon him in the interests of orderly administration and discipline of the service.<sup>186</sup>

5.137 Higgins J of the ACT Supreme Court expressed a contrasting view, stating that some limitations could be implied into s 70:

Whether a duty of confidentiality arises so that s 70 *Crimes Act* can punish its breach will depend on the type of information, the circumstances in which it has been acquired and the interests of relevant parties in keeping it confidential. A consideration of the public interest must also be relevant. The duty to keep information confidential may attach to information of any kind but it must be such and acquired in such circumstances that such a duty arises. It does not arise merely because the information is obtained by an officer in the course of his or her duties.<sup>187</sup>

5.138 The application of s 70 to the disclosure of information will depend on the nature of the duty not to disclose. For example, the equitable duty of confidentiality only arises where the disclosure would be inimical to the public interest.<sup>188</sup> Therefore, a prosecution for an offence under s 70, reliant on a breach of an equitable or common law duty to protect confidential information, may require the prosecution to show that the disclosure was likely to harm the public interest. On the other hand, if the prosecution relied upon a breach of a statutory duty not to disclose any information

<sup>184</sup> *Cortis v R* [1978] WAR 30, 32. See also J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 52–53.

<sup>185</sup> L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 259.

<sup>186</sup> *Commissioner of Taxation v Swiss Aluminium Australia Ltd* (1986) 10 FCR 321, 325.

<sup>187</sup> *Deacon v Australian Capital Territory* [2001] ACTSC 8, [87]–[88].

<sup>188</sup> *Commonwealth v Fairfax* (1980) 147 CLR 39.

obtained in the course of employment, s 70 could potentially apply to the disclosure of information already in the public domain.<sup>189</sup>

5.139 Section 70 expressly applies to the communication or publication of a ‘fact or document’. Neither ‘fact’ nor ‘document’ is defined. Finn has argued that the need for disclosure of a ‘fact or document’, rather than ‘information’, opens the application of s 70 to anomalies:

Where a document is not disclosed all that is protected is a ‘fact’; where a document is disclosed its contents need not be ones of fact. Unless ‘fact’ is given a meaning which covers disclosure of advice, opinion, intention etc, the scope of the offence is manipulated simply by the particular means (oral or documentary) used in the disclosure.<sup>190</sup>

5.140 The distinction between the communication of a fact or a document can be important to the prosecution of an offence. In *R v Kessing*, a former officer of the Australian Customs Service, Allan Kessing, was convicted of providing reports about airport security arrangements to two journalists.<sup>191</sup> On appeal, the New South Wales Court of Criminal Appeal held that the trial judge had misdirected the jury in saying that it was sufficient if the prosecution could establish that Kessing had confirmed the accuracy of material that journalists had obtained from another source. Bell JA, with whom Rothman and Price JJ agreed, stated that:

The offence under s 70 may be committed by publishing or communicating a fact which came to the knowledge of the accused by virtue of having been a Commonwealth officer or by publishing or communicating a document which came into his or her possession by virtue of having been a Commonwealth officer or by both. This was a case in which the offence charged was the communication of the documents. To confirm the accuracy of a document leaked by another to a journalist may be to communicate a fact, but in my opinion it is not to communicate the document.<sup>192</sup>

5.141 Further, Tsaknis has pointed out that it is unclear whether the release of any information would constitute a ‘fact’ or whether the prosecution needs to prove the factual accuracy of the information in order to satisfy the terms of s 70 of the *Crimes Act*.<sup>193</sup>

### ***What kind of activity is regulated?***

5.142 A person commits an offence under s 70 if he or she ‘publishes or communicates ... any fact or document’. The *Crimes Act* does not provide any guidance as to the meaning of the term ‘publishes or communicates’. In *Kessing v The*

---

189 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 216.

190 Ibid, 212–213.

191 *R v Kessing* [2007] NSWDC 138.

192 *Kessing v The Queen* [2008] NSWCCA 310, [61].

193 L Tsaknis, ‘Commonwealth Secrecy Provisions: Time for Reform?’ (1994) 18 *Criminal Law Journal* 254, 261.

*Queen*, Bell JA, with whom Rothman and Price JJ agreed, summarised this requirement as follows:

To ‘communicate’ is to transmit or to impart knowledge or make known (*Macquarie Concise Dictionary*, 3rd ed.) One may ‘communicate’ a document by communicating the contents of the document. This is how the Crown particularised this case. Generally, to publish connotes to make publicly known, however, in the law of defamation publication applies to making the matter complained of known to any person other than the person defamed.<sup>194</sup>

5.143 Further, Bell JA confirmed that communication for the purposes of s 70 can be direct or indirect:

Communication of the contents of a document requires no more than that the contents be conveyed or transmitted to another. This may be done directly by handing the document to another or by reading the document to another. It may be done indirectly by leaving the document on a park bench for another to collect or in any of a variety of ways. The essential feature of communicating a fact or document for the purposes of s 70 is that the communication is intentional.<sup>195</sup>

### ***Whose activity is regulated?***

5.144 Section 70(1) of the *Crimes Act* applies to Commonwealth officers, while s 70(2) applies to former Commonwealth officers. The definition of Commonwealth officer set out in s 3 of the *Crimes Act* includes a person:

- appointed or engaged under the *Public Service Act*;
- employed in the public service of a territory, ADF, AFP or public authority under the Commonwealth;
- who performs services for or on behalf of the Commonwealth, a territory or public authority; and
- who performs services, or is an employee of the Australian Postal Corporation.

5.145 The list of persons included in this definition is not exhaustive, and some categories could be broadly interpreted. In particular, ‘a person holding office under, or employed by, the Commonwealth’ arguably includes a very wide category of persons. While there has been little judicial consideration of who may be considered a Commonwealth officer, judges,<sup>196</sup> ministers<sup>197</sup> and ministerial staff all potentially fall

<sup>194</sup> *Kessing v The Queen* [2008] NSWCCA 310, [31].

<sup>195</sup> *Ibid*, [36].

<sup>196</sup> See comments by Gummow J in *Grollo v Palmer* (1995) 184 CLR 348, 396.

<sup>197</sup> There is some uncertainty about whether a minister is a Commonwealth officer for the purposes of the *Crimes Act*. The *Migration Act 1958* (Cth) s 503A(9) defines ‘Commonwealth officer’ as having the same meaning as in s 70 of the *Crimes Act 1914* (Cth), but includes a note that ‘a Minister is not a Commonwealth officer’.

within the definition. It is important to note that while a person may be a Commonwealth officer, it does not necessarily follow that they have a duty not to disclose information—for example, judges exercising federal judicial power may not be bound by such a duty.<sup>198</sup>

5.146 Other legislation may deem certain officers to be Commonwealth officers. For example, officers or employees of ASIO<sup>199</sup> and staff members of the Australian Secret Intelligence Service<sup>200</sup> are deemed to be Commonwealth officers for the purposes of the *Crimes Act*.

#### ***Exception—Authorised disclosures***

5.147 Section 70(1) includes an exception to the offence where the person discloses the information ‘to some person to whom he or she is authorised to publish or communicate it’. Section 70(2) contains a different exception to the offence, in that the publication or communication must be ‘without lawful authority or excuse’, proof of which lies with the defendant.

5.148 The scope of each exception, and the extent of any difference between them, is unclear. If the duty not to disclose arises under a particular statutory provision, that provision may make clear the circumstances in which publication or communication of information is authorised. In relation to s 70(1), Tsaknis has suggested that the statute conferring functions, powers and duties conferred on a Commonwealth officer by particular legislation may provide an implied authority to release information.<sup>201</sup> Similarly, in relation to s 70(2), the common law may provide a ‘lawful excuse’, particularly where the ‘duty not to disclose’ arises under contractual, common law or equitable principles.<sup>202</sup>

5.149 Section 70 does not create an exception or defence relating to disclosure in the public interest. However, it is possible that this kind of ‘justification’ might be considered in sentencing in a particular case.<sup>203</sup>

#### **Section 79—disclosure of official secrets**

5.150 Section 79 of the *Crimes Act* creates a number of offences relating to the use or disclosure of official secrets. A version of s 79 formed part of the first *Crimes Act* in 1914 and was based on provisions of the *Official Secrets Act 1911* (UK).<sup>204</sup> While s 79

---

198 Issues relating to the application of secrecy provisions to judicial officers are discussed in Chs 2 and 8.

199 *Australian Security Intelligence Organisation Act 1979* (Cth) s 91.

200 *Intelligence Services Act 2001* (Cth) s 38.

201 L Tsaknis, ‘Commonwealth Secrecy Provisions: Time for Reform?’ (1994) 18 *Criminal Law Journal* 254, 261.

202 P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 259.

203 See, eg, comments of Bennett SC DJC in *R v Kessing* [2007] NSWDC 138, [49]–[63].

204 Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney-General), 265.

deals with espionage offences, there is also significant overlap with the general secrecy offence in s 70. Section 79 is set out in full in Appendix 5.

5.151 There have been few prosecutions under s 79. One example is the conviction, in 2003, of Simon Lappas of offences under s 79(3) and s 78 of the *Crimes Act* (which was subsequently repealed and replaced by s 91.1 of the *Criminal Code*). Lappas, an employee of the Defence Intelligence Organisation, had given several classified documents to an unauthorised person, Sherryl Dowling, so she could sell the documents to a foreign power.<sup>205</sup> Lappas was found guilty and, on appeal, sentenced to two years' imprisonment. Dowling pleaded guilty to two charges of receiving the classified documents and was placed on a five year good behaviour bond.<sup>206</sup>

5.152 Another example is the conviction in 1977 of a probationary trainee of ASIO, of offences under s 79(3). He had communicated official secrets as part of a 'personal practical experiment' to see what kind of response he would get to an overture to a foreign agency purporting to offer intelligence secrets.<sup>207</sup>

#### ***What kind of information is protected?***

5.153 Section 79 can be categorised as both a general and a specific secrecy provision, depending on the kind of information disclosed. Section 79(1) defines three categories of information covered by the offence.

5.154 Sections 79(1)(a) and (c) set out two categories dealing with the disclosure of particular kinds of defence and security information—information made or obtained in contravention of pt VIII of the *Crimes Act* (ie, by unlawful soundings) or s 91.1 of the *Criminal Code* (ie, by espionage) and information relating to a prohibited place. Where s 79 is used in relation to this kind of information, it can be categorised as a specific secrecy provision protecting defence or security information. This aspect is discussed above in relation to secrecy provisions that protect defence or security information.

5.155 The third category of information covered by s 79 is more general in application. Section 79(1)(b) defines protected information as information which

has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he or she has made or obtained it owing to his or her position as a person:

- (i) who is or has been a Commonwealth officer;
- (ii) who holds or has held office under the Queen;

---

205 *R v Lappas* (2003) 152 ACTR 7.

206 Transcript of Proceedings, *R v Dowling*, (Supreme Court of the Australian Capital Territory, Gray J, 9 May 2003). The factual background to the Lappas and Dowling cases, and an outline of the court proceedings, are set out in Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Appendix 4.

207 *Grant v Headland* (1977) 17 ACTR 29.

- (iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth;
- (iv) who is or has been employed by or under a person to whom a preceding subparagraph applies; or
- (v) acting with the permission of a Minister;

and, by reason of its nature or the circumstances under which it was entrusted to him or her or it was made or obtained by him or her or for any other reason, it is his or her duty to treat it as secret.<sup>208</sup>

5.156 The category of information protected by s 79(1)(b) is similar to that in s 70, insofar as it does not create a duty to keep information confidential, but relies on a ‘duty to treat [the information] as secret’. As with s 70, this duty could stem from the common law, a statutory secrecy provision or the terms of a contract. However, s 79 is not necessarily dependent on a statutory or legal duty arising from a person’s position as a Commonwealth officer. Because the offences cover ‘any person’, s 79 contemplates that a duty to keep information secret could arise from the nature of the information—for example, a document that was headed with a security classification—or the circumstances in which the information was obtained.

5.157 The information covered by s 79 can take the form of a ‘sketch, plan, photograph, model, cipher, note, document, or article’. ‘Article’ is defined to include ‘any thing, substance or material’; while information is broadly defined to mean ‘information of any kind whatsoever, whether true or false and whether in a material form or not, and includes (a) an opinion; and (b) a report of a conversation’.

5.158 In common with s 70, s 79 applies to all information, regardless of its nature or the effect of its disclosure. As noted by the review of Commonwealth criminal law by the committee chaired by Sir Harry Gibbs in 1991:

No distinction is drawn for the purposes of these provisions between information the disclosure of which may cause real harm to the public interest and information the disclosure of which may cause no harm whatsoever to the public interest.<sup>209</sup>

5.159 Not all material or information that falls within the existing definition of ‘official secrets’ would harm the public interest if disclosed. Information may have been obtained in contravention of s 79, for example, but may no longer be sensitive due to the passage of time or prior disclosure in Australia or overseas. Nevertheless, communicating this information may still constitute an offence under s 79.

---

208 *Crimes Act 1914* (Cth) s 79(1)(b).

209 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 242.

***What kind of activity is regulated?***

5.160 Section 79 creates a number of offences relating to the use and disclosure of ‘prescribed information’ (for convenience, here referred to as an ‘official secret’). The offences can be summarised as follows:

- s 79(2): communicating or allowing someone to have access to or retaining an official secret without authorisation with ‘the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen’s dominions’—maximum penalty seven years imprisonment.
- s 79(3): communicating or allowing someone to have access to an official secret without authorisation—maximum penalty two years imprisonment.
- s 79(4): retaining, failing to comply with a direction regarding the retention or disposal of an official secret, failing to take reasonable care of prescribed information or conducting oneself as to endanger its safety—maximum penalty six months imprisonment.
- s 79(5): receiving information knowing or having reasonable ground to believe, at the time when he or she receives it, that the information is communicated to him or her in contravention of s 91.1 of the *Criminal Code* or s 79(2)—maximum penalty seven years imprisonment.
- s 79(6): receiving information knowing or having reasonable ground to believe, at the time when he or she receives it, that the information is communicated to him or her in contravention of s 79(3)—maximum penalty two years imprisonment.

5.161 A notable aspect of s 79 is that the mere receipt of information can constitute a criminal offence. By way of background, the *Criminal Code Amendment (Espionage and Related Matters) Act 2002* repealed and replaced the espionage offences originally in pt VII of the *Crimes Act*. The Criminal Code Amendment (Espionage and Related Offences) Bill 2001 (Cth) was initially intended also to repeal and replace s 79 of the *Crimes Act* with updated provisions in the *Criminal Code*, although the new provisions did not exactly replicate s 79. In particular, the new offence of ‘receiving certain information’ did not require the person to know or have reasonable grounds to believe that the information was communicated in contravention of the espionage or secrecy provisions.<sup>210</sup>

---

210      Criminal Code Amendment (Espionage and Related Offences) Bill 2001 (Cth) cl 82.4.

5.162 The new provisions were criticised—particularly by media organisations—on the basis that the provisions would interfere with freedom of speech and prevent public discussion of important issues of public interest.<sup>211</sup> As a result, the provisions intended to replace s 79 were removed from the Bill. The then Attorney-General, the Hon Daryl Williams AM QC MP, explained this decision as follows:

Recently concerns have been raised about the official secrets provisions in that bill. ... There has been considerable media attention focused on the perceived impact that the official secrets provisions in the earlier bill were alleged to have on the freedom of speech and on the reporting of government activities.

The original bill did not alter the substance of the official secrets offences; it simply modernised the language of the offences consistent with the *Criminal Code*. The government's legal advice confirms that there was in substance no difference between the current provisions of the *Crimes Act* and the proposed provisions of the *Criminal Code*. The allegations ignore the fact that the existing law has not prevented the reporting of such stories in the past. Despite this, to avoid delay in the reintroduction of the important espionage provisions, the government decided to excise the official secrets provisions from the bill so only those relating to espionage have been included in the bill introduced today.<sup>212</sup>

### ***Whose activity is regulated?***

5.163 Section 79 is not confined to the actions of Commonwealth officers or former Commonwealth officers. The offences cover the communication, receipt or handling of an official secret by any person. The offence applies regardless of whether the person was aware that he or she had a duty not to disclose information.<sup>213</sup> However, the circumstances in which a third party who is not a Commonwealth officer can be said to have a *duty* to keep information secret are not clear.

### ***Exceptions and defences***

5.164 Sub-sections 79(2) and (3) permit the disclosure of prescribed information to:

- (a) a person to whom he or she is authorized to communicate it; or
- (b) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it.

5.165 The exemption regarding a duty to communicate information ‘in the interests of the Commonwealth’ is based on s 2(1) of the (now repealed) *Official Secrets Act 1911* (UK). The exemption was considered by a United Kingdom court in the case of *R v Ponting*.<sup>214</sup> Mr Ponting was a senior civil servant in the Ministry of Defence. In preparing a briefing for the Minister, Ponting saw documents which showed that the

211 R Sharman, ‘Espionage and Related Offences Bill’ (2002) 21(1) *Communications Law Bulletin* 7, 8.

212 Commonwealth, *Parliamentary Debates*, House of Representatives, 13 March 2002, 1111 (A-G The Hon Daryl Williams AM QC MP); Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Criminal Code Amendment (Espionage and Related Offences) Bill 2002* (2002), 1.

213 *Grant v Headland* (1977) 17 ACTR 29, 31.

214 *R v Ponting* [1985] Crim LR 318.

government had provided incorrect information to Parliament about the sinking of the Argentinian ship *Belgrano* during the Falklands War. When the Minister did not correct the information, Ponting provided copies of the documents to an Opposition Member of Parliament. He was charged under the *Official Secrets Act 1911* (UK).

5.166 In his defence, Ponting argued that he had disclosed the documents ‘in the interests of the state’, the equivalent exception to that contained in s 79(3)(b) of the *Crimes Act*. At trial, the judge gave a direction to the jury that the reference to this duty was to an official duty rather than a moral, contractual or civic duty, and the ‘interests of the state’ were the interests according to its recognised organs of government and the policies as expounded by the particular government of the day.<sup>215</sup>

5.167 It is not necessarily the case that an Australian court would interpret s 79(2)(b) and (3)(b) in the same way, particularly given the High Court’s decision in *Commonwealth v Fairfax*,<sup>216</sup> which set out factors relevant to determining the public interest in the confidentiality and disclosure of certain information.<sup>217</sup>

5.168 Subsections 79(5) and (6) provide that a person is not guilty of an offence of receiving prescribed information if he or she can prove that the ‘communication was contrary to his or her desire’.

## Comment

5.169 There is some overlap between ss 70 and 79 of the *Crimes Act*. This may reflect the different sources of each provision—as noted above, s 70 is based on a provision of the *Criminal Code Act 1899* (Qld), while s 79 is based on provisions of the (now repealed) *Official Secrets Act 1911* (UK).

5.170 In particular, there are considerable similarities and points of overlap between ss 70 and 79(3) of the *Crimes Act*. The offence under s 79(3), which does not require communication with an intention to prejudice the security or defence of the Commonwealth, appears to apply to the same broad range of information covered by s 70. Both provisions apply criminal sanctions to the breach of a ‘duty’ that is found either outside the criminal provision (ss 70 and 79(3)) or determined by the nature of the information or circumstances of the communication (s 79(3)).

5.171 However, s 70 applies only to Commonwealth officers who publish or communicate information, while s 79(3) applies to ‘any person’ who communicates or permits access to protected information. Further, s 79(6) applies to any person who receives information, knowing or having reasonable grounds to believe, that the information was communicated in contravention of s 79(3).

<sup>215</sup> Ibid. The jury nevertheless found Ponting not guilty.

<sup>216</sup> *Commonwealth v Fairfax* (1980) 147 CLR 39.

<sup>217</sup> L Tsaknis, ‘Commonwealth Secrecy Provisions: Time for Reform?’ (1994) 18 *Criminal Law Journal* 254, 266.

5.172 A further point of difference between the two provisions is that s 79(3)(b) contains an exception that permits a person to communicate information ‘in the interests of the Commonwealth’. The meaning and scope of this exception is unclear. Tsaknis has suggested that it is possible that a disclosure may be justified under s 79 in the interests of the Commonwealth and yet prohibited under s 70.<sup>218</sup>

5.173 Both ss 70 and 79(3) of the *Crimes Act* operate as ‘catch-all’ provisions to criminalise the disclosure of a potentially wide variety of information in breach of some other duty. Because the offences are contingent on duties found beyond the terms of those offences, there is great potential for uncertainty about the kind of conduct that will attract criminal sanctions.

5.174 Chapter 6 considers the effectiveness of the general secrecy offences in ss 70 and 79(3), while Chapters 7, 8 and 9 consider how the general secrecy offences currently in the *Crimes Act* can be updated and improved.

5.175 The overview in this chapter also reveals a number of key areas for further examination in relation to specific secrecy provisions, particularly where those provisions create offences. Chapters 10, 11 and 12 examine the appropriate elements of specific secrecy offences and suggest how such offences can be simplified and drafted in a consistent manner. In particular, in reviewing both the general and specific secrecy offences, the ALRC has been concerned to test secrecy laws against identifiable public interests with an emphasis on identifying and protecting against the harm that the disclosure of information may cause.

---

218 Ibid.



# 6. The Need for a General Secrecy Offence

---

## Contents

Introduction	199
Criminal, civil or administrative penalties	200
Administrative penalties	201
Civil penalties	203
Criminal penalties	208
The need for a general secrecy offence	216

## Introduction

6.1 In Chapter 5, the ALRC considers general law obligations—such as an employee’s duty of loyalty and fidelity and the equitable duty of confidence—and the extent to which they protect Commonwealth information in the hands of Commonwealth officers and others from unauthorised disclosure. The ALRC has concluded that these general law obligations do not provide sufficient protection in the public sector context, and that it is necessary and desirable to have in place certain statutory provisions that impose obligations on Commonwealth officers and others who handle Commonwealth information. This chapter examines the potential role of administrative, civil and criminal statutory provisions in regulating the disclosure of Commonwealth information.

6.2 In addition, in the Issues Paper, *Review of Secrecy Laws* (IP 34),<sup>1</sup> the ALRC sought stakeholder views on whether the unauthorised handling of Commonwealth information should remain subject to a general criminal offence—such as the existing ss 70 and 79(3) of the *Crimes Act 1914* (Cth)—updated and moved to the *Criminal Code* (Cth),<sup>2</sup> and, if so, how such an offence should be framed.<sup>3</sup> The ALRC is of the view that there is a role for both administrative and criminal penalties in this area and proposes that ss 70 and 79(3) of the *Crimes Act* should be repealed and replaced by a new general secrecy offence in the *Criminal Code*.

6.3 Chapters 7 to 9 go on to consider some of the essential elements of the proposed new offence. The key element in the ALRC’s proposed general secrecy offence is that

---

<sup>1</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

<sup>2</sup> Ibid, Question 2–1.

<sup>3</sup> Ibid, Question 2–2.

the prosecution should be required to prove that a particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to specified public interests, such as the security or defence of the Commonwealth. In the absence of any likely, intended or actual harm to those public interests, the ALRC has formed the preliminary view that the unauthorised disclosure of Commonwealth information is more appropriately dealt with by the imposition of administrative penalties or the pursuit of contractual remedies.<sup>4</sup>

## Criminal, civil or administrative penalties

6.4 As discussed in Chapter 5, there are many existing statutory provisions that impose secrecy obligations and carry a range of administrative, civil or criminal penalties. However, of the 507 secrecy provisions identified by the ALRC,<sup>5</sup> about 70% impose criminal penalties. The majority of the remaining provisions do not expressly contain criminal penalties, but by establishing a duty not to disclose Commonwealth information, they have the potential to attract the penalties imposed by s 70 of the *Crimes Act*.<sup>6</sup>

6.5 A number of secrecy provisions allow the imposition of administrative sanctions—such as termination of employment, a reduction in salary or a reprimand—on public sector employees. For example, s 15 of the *Public Service Act 1999* (Cth) allows an Australian Government agency head to impose a range of administrative sanctions on Australian Public Service (APS) employees for breach of the APS Code of Conduct. As discussed in detail in Chapter 13, the Code of Conduct includes a secrecy provision that prohibits the disclosure of information obtained or generated in connection with an APS employee’s employment ‘if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government’.<sup>7</sup>

6.6 Finally, the ALRC has identified three secrecy provisions that impose civil penalties. Two of these provisions are found in the *Workplace Relations Act 1996* (Cth)<sup>8</sup> and one in the *Environment Protection and Biodiversity Conservation Act 1998* (Cth).<sup>9</sup>

6.7 In weighing up what penalties might be appropriate, regulatory theory cautions against the over-use of criminal penalties. Criminal penalties sit at the top of the ‘enforcement pyramid’ developed by Ayers and Braithwaite to describe a model

<sup>4</sup> Administrative penalties and contractual remedies are considered in detail in Chs 12 and 13.

<sup>5</sup> See Appendix 4.

<sup>6</sup> Section 70 of the *Crimes Act* and the need to establish an external ‘duty not to disclose’ are described in Ch 5 and considered further in Ch 7.

<sup>7</sup> *Public Service Regulations 1999* (Cth) reg 2.1, read with *Public Service Act 1999* (Cth) s 13(13). Other provisions imposing administrative sanctions include the *Cadet Force Regulations 1977* (Cth) sch 4 cl 5 read with ss 16 and 17; and the *Parliamentary Service Act 1999* (Cth) s 13(6) read with s 15.

<sup>8</sup> *Workplace Relations Act 1996* (Cth) s 715 and sch 1 s 276.

<sup>9</sup> *Environment Protection and Biodiversity Conservation Act 1998* (Cth) s 170B.

regulatory approach.<sup>10</sup> Under the ‘enforcement pyramid’ model, breaches of increasing seriousness are dealt with by penalties of increasing severity, with the ultimate penalties—such as imprisonment—held in reserve. Braithwaite has described the operation of the pyramid in the regulatory environment as follows:

My contention is that compliance is most likely when the regulatory agency displays an explicit enforcement pyramid … Most regulatory action occurs at the base of the pyramid where initially attempts are made to coax compliance by persuasion. The next phase of enforcement escalation is a warning letter; if this fails to secure compliance, civil monetary penalties are imposed; if this fails, criminal prosecution ensues; if this fails, the plant is shut down or a licence to operate is suspended; if this fails, the licence to do business is revoked … The form of the enforcement pyramid is the subject of the theory, not the content of the particular pyramid.<sup>11</sup>

6.8 Although this model was developed in the corporate regulatory environment, the principles of the enforcement pyramid model are still broadly applicable to the issues under consideration in this Inquiry. At the bottom of the enforcement pyramid lie the techniques described in Chapter 15, which are designed to foster a culture in which Commonwealth information is handled effectively—such as agency policies and guidelines, staff training and development, and secrecy oaths and affirmations. Where these techniques fail to prevent unauthorised disclosure, administrative penalties, or general law or contractual remedies may be available. Where the disclosure is more serious—for example, where the disclosure has the potential to cause serious harm or is intended to cause harm—criminal penalties may be applied.

6.9 In IP 34, the ALRC asked for stakeholder views on when it is appropriate to impose administrative penalties for the unauthorised handling of Commonwealth information,<sup>12</sup> and when it is appropriate to impose criminal penalties.<sup>13</sup> The ALRC also asked whether civil penalties should have a greater role to play in protecting Commonwealth information.<sup>14</sup> In the following section, the ALRC considers the role of administrative, civil and criminal penalty provisions in protecting Commonwealth information.

### Administrative penalties

6.10 Broadly speaking, administrative penalties arise automatically by operation of legislation, or can be imposed directly by an agency or regulator—for example, parking fines. This distinguishes them from criminal and civil penalties, which may

---

10 The model was first put forward by Braithwaite in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985). See also I Ayers and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992).

11 Quoted in F Haines, *Corporate Regulations: Beyond ‘Punish or Persuade’* (1997), 218–219.

12 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–13.

13 Ibid, Question 5–1.

14 Ibid, Question 5–17.

only be imposed by courts.<sup>15</sup> In the public sector context, Commonwealth employees will often be subject to secrecy obligations, breach of which may result in the imposition of administrative penalties by an agency head.

6.11 For example, as considered in detail in Chapter 13, where an APS employee breaches the Code of Conduct in the *Public Service Act*, an agency head may impose one of the following penalties: termination of employment; reduction in classification; re-assignment of duties; reduction in salary; deductions from salary (which are not to exceed 2% of the APS employee's annual salary);<sup>16</sup> or a reprimand.<sup>17</sup> While some of these penalties, such as termination of employment, are quite severe, they are considered disciplinary rather than criminal in nature.

6.12 Further, an APS employee who commits a secrecy offence will also automatically be in breach of the APS Code of Conduct, which requires APS employees to comply with all applicable Australian laws. In these circumstances, APS employees will be liable to both criminal and administrative penalties for the same conduct.

6.13 Administrative penalties under the *Public Service Act*, and other similar legislation,<sup>18</sup> apply to current Commonwealth employees. They do not apply to former employees or persons in the private sector who may have access to Commonwealth information. For example, a person who retires from the APS, or resigns when an investigation into a suspected breach of the Code of Conduct commences, is no longer subject to administrative penalties under the *Public Service Act*. Former employees, however, remain liable to criminal penalties under the *Crimes Act* and, potentially, a range of other provisions.

6.14 In Chapters 13 and 14, the ALRC considers in detail the role of secrecy provisions that impose administrative penalties on public sector employees. The secrecy requirements set out in the APS Code of Conduct, and in other similar instruments, are a 'public statement of the standards of behaviour expected of those who work in public employment'.<sup>19</sup>

6.15 In the ALRC's view such provisions have an important role to play, particularly where a disclosure is inadvertent, there is no intention to cause harm, or where any potential harm caused by the disclosure is likely to be minor. Administrative penalties

15 Under the *Australian Constitution*, and the doctrine of the separation of powers, only judicial officers may exercise the judicial power of the Commonwealth, including the imposition of fines: *R v White; Ex Parte Byrnes* (1963) 109 CLR 665, 669–670, or other punishment for an offence: *Federal Commissioner of Taxation v Munro* (1926) 38 CLR 153, 175.

16 *Public Service Act 1999* (Cth) s 15; *Public Service Regulations 1999* (Cth) reg 2.3.

17 *Public Service Act 1999* (Cth) s 15.

18 *Parliamentary Service Act 1999* (Cth); *Defence Force Discipline Act 1982* (Cth); *Australian Federal Police Act 1979* (Cth); *Cadet Force Regulations 1977* (Cth).

19 P Shergold, 'A New Public Service Act: The End of the Westminster Tradition?' (1997) 85 *Canberra Bulletin of Public Administration* 32, 34.

provide a range of responses to different levels of misconduct. They allow misconduct of a lower order to be addressed in the employment context, without imposing the very serious consequences of a criminal charge and conviction, consistent with the enforcement pyramid model.

6.16 In Chapters 13 to 15, the ALRC considers how administrative secrecy provisions, and the methods for enforcing those provisions, could be improved. The ALRC's view is, however, that such provisions are, and should remain, an important and effective element in the protection of Commonwealth information. In Chapter 14, the ALRC makes a number of proposals to ensure that individuals who fall outside the various administrative regimes but have, or have had, access to Commonwealth information are constrained by contractual obligations, or are made aware of their obligations of confidentiality under the general law.

### Civil penalties

6.17 As noted above, the ALRC has identified three secrecy provisions that impose civil penalties:

- s 276 of sch 1 of the *Workplace Relations Act* provides that a member of a registered organisation of employers or employees, who has obtained an order from the Australian Industrial Relations Commission (AIRC) to allow the member to inspect the financial records of the organisation, must not disclose information acquired from that inspection except to certain specified persons;<sup>20</sup>
- s 715 of the *Workplace Relations Act* provides that a person who conducts a dispute resolution process under the Act—where the process is not conducted by the AIRC—must not disclose information obtained in the course of the process except in specified circumstances,<sup>21</sup> and
- s 170B of the *Environment Protection and Biodiversity Conservation Act* allows the Minister to issue a direction to any person prohibiting the disclosure of 'specified information' in documents or materials required or permitted to be published as part of an environmental impact assessment process. Specified information is that which the Minister considers to be critical to the protection of a matter of national environmental significance.<sup>22</sup>

---

20 The maximum pecuniary penalty for breach of this provision is, in the case of a body corporate, 100 penalty units (currently \$11,000) and in any other case, 20 penalty units (currently \$2,200): *Workplace Relations Act 1996* (Cth) sch 1 s 306.

21 Ibid s 715(6) provides that the maximum pecuniary penalty for breach of this provision is, in the case of a body corporate, 300 penalty units (currently \$33,000) and in any other case, 60 penalty units (currently \$6,600).

22 The maximum pecuniary penalty for breach of this provision is 100 penalty units (currently \$11,000).

6.18 Traditionally, the civil law has been used as a vehicle for private redress, allowing persons to seek compensation in private actions for harm done to them. Modern regulatory law, however, has created many civil penalty provisions. Contraventions of these provisions are pursued by the state, but are not criminal offences and do not attract criminal processes or penalties.<sup>23</sup>

6.19 Most civil penalties are monetary. The maximum financial penalty under a civil penalty provision can be higher than the maximum fine for a parallel criminal offence. This is justified on the basis that the adverse effects of a criminal conviction should be taken into account when considering the relative severity of criminal and civil financial penalties.<sup>24</sup> Civil penalty provisions may also provide for the imposition of compensation orders<sup>25</sup> or community service orders.<sup>26</sup> They may also allow the court to issue an injunction, which is not in itself a penalty, but may act to prevent or limit any potential harm caused by the contravention.

6.20 The procedures and rules of evidence in civil cases apply to the enforcement of civil penalty provisions. In criminal proceedings the prosecution must prove its case beyond reasonable doubt.<sup>27</sup> The standard of proof in civil proceedings is on the balance of probabilities.<sup>28</sup>

6.21 The Australian Government Attorney-General's Department (AGD) *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that:

It is particularly important that civil penalties be used in appropriate and justifiable contexts. They are otherwise open to criticism for being too soft (in not carrying a criminal penalty) or for being too harsh (in not carrying the safeguards of criminal procedure such as a requirement for proof beyond reasonable doubt).<sup>29</sup>

6.22 Taking into account recommendations made by the ALRC in its report on civil and administrative penalties,<sup>30</sup> the *Guide to Framing Commonwealth Offences* nominates the following criteria as relevant to whether a civil penalty provision is likely to be appropriate and effective:

---

23 See Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 62.

24 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 26–3; Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 66.

25 *Corporations Act 2001* (Cth) ss 1317H, 1317HA; *Trade Practices Act 1974* (Cth) s 87.

26 *Trade Practices Act 1974* (Cth) s 86C.

27 *Evidence Act 1995* (Cth) s 141.

28 *Ibid* s 140.

29 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 63.

30 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002).

- where criminal punishment is not warranted—contraventions of the law involving serious moral culpability should only be pursued by criminal prosecution;
- where the maximum civil penalty is sufficient to justify the expense and time of court proceedings—the maximum penalty should be at least \$5,000 and typically more; and
- where the conduct involves corporate wrongdoing—given that imprisonment is not available as a penalty, the financial disincentives that civil penalties offer may be effective.<sup>31</sup>

6.23 Civil penalties are used extensively, for example, in relation to contraventions of pt IV of the *Trade Practices Act 1974* (Cth), dealing with restrictive trade practices; and in relation to contraventions of a significant number of provisions in the *Corporations Act 2001* (Cth).<sup>32</sup> Another example, of more direct relevance to this Inquiry, is s 25 of the *Commonwealth Authorities and Companies Act 1997*—which imposes civil penalties on officers and employees of Commonwealth authorities for improperly using information: to gain an advantage for themselves or another person; or to cause detriment to a Commonwealth authority or to another person.

6.24 Professor Arie Freiberg suggests that civil penalty provisions may be effective where there is an ongoing regulatory relationship:

The greater flexibility and range of civil sanctions makes them the preferred mode of social control where persuasion, negotiation and voluntary compliance are viewed as the techniques most likely to achieve the desired results. Whilst the criminal sanction is said to be suitable for the control of isolated or instantaneous conduct, the civil sanction is said to be better in cases where continuous surveillance is desired.<sup>33</sup>

### ***Submissions and consultations***

6.25 Although the response in submissions to the use of civil penalty provisions was mixed, the weight of opinion was in favour of criminal, rather than civil, penalties. In its submission, the AGD noted that civil penalties may be used when criminal punishment is not merited, but expressed the view that, given the nature of the information protected by secrecy provisions, criminal sanctions would generally be appropriate.<sup>34</sup> The Australian Taxation Office (ATO) also expressed the view that, in the taxation arena, the unauthorised handling of taxpayer information should be subject to criminal penalties:

---

31 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 63–64.

32 *Corporations Act 2001* (Cth) pt 9.4B.

33 A Freiberg, ‘Civilizing Crime’: Reactions to Illegality in the Modern State, *Thesis*, 1985, 120.

34 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

Nevertheless, the ATO recognises that there may be varying degrees of culpability associated with the unauthorised handling of tax information, that criminal prosecution is a very serious consequence, and that the criminal standard of proof can be onerous to satisfy. In addition to criminal sanctions, there may be some merit in having civil options available for breach of a tax secrecy provision, as well as Code of Conduct action under the *Public Service Act*.<sup>35</sup>

6.26 The Public Interest Advocacy Centre (PIAC) submitted that disclosures that do not involve intent to damage a significant public interest—such as defence or national security—and that do not involve an element of fraud, dishonesty, or personal gain should be dealt with under civil penalty provisions.<sup>36</sup>

6.27 On the other hand, the Australian Prudential Regulation Authority (APRA) expressed the view that when there is already a criminal regime in place, civil penalties add little—and that the deterrence value of criminal penalties was important.<sup>37</sup> Liberty Victoria agreed, stating that:

A civil penalty for the deliberate mishandling of non [National Security Information] for significant gain may be an insufficient deterrent. This is particularly so where the maximum civil penalty is outweighed by a substantial commercial benefit.<sup>38</sup>

6.28 James Renwick drew attention to the utility of civil remedies in dealing with disclosure of Commonwealth information, and suggested that such matters would be more effectively dealt with in civil, rather than criminal, courts:

Although criminal prosecution must remain an option to deter theft or leaking of that information, it is often a blunt instrument, which takes too much time. In contrast the civil litigation system properly used permits the swift quarantining of information and delivery up of any stolen material. A criminal law sanction will not normally be interpreted as permitting a court exercising civil jurisdiction to grant injunctions or other civil relief. It is therefore essential that there be an effective statutory regime for protecting stolen or leaked information in the civil courts. The Federal Court of Australia would be the appropriate forum for such litigation.<sup>39</sup>

6.29 The AGD expressed support for including a power to issue injunctions in secrecy provisions but noted that an injunction would be of limited assistance in relation to the disclosure of Commonwealth information because it is rare to have forewarning of an unauthorised disclosure. In addition, the AGD stated that compensation orders may be problematic because such orders usually require the quantification of the loss or damage caused. This is often difficult in relation to the unauthorised disclosure of Commonwealth information, ‘for example, it would be

---

35 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

36 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

37 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

38 Liberty Victoria, *Submission SR 19*, 18 February 2009.

39 J Renwick, *Submission SR 02*, 11 December 2008.

difficult to assess and quantify the damage to the integrity of the Cabinet process caused by disclosure of a Cabinet document'.<sup>40</sup>

#### **ALRC's views**

6.30 Although civil penalty provisions exist among the hundreds of secrecy provisions identified by the ALRC,<sup>41</sup> such provisions are quite uncommon and, therefore, appear somewhat anomalous.

6.31 The conduct of public sector employees who handle Commonwealth information is largely regulated by administrative secrecy provisions, in conjunction with the criminal law. Administrative penalties are available because of the employment relationship between Australian Government agencies and their employees. This relationship does not exist between regulatory authorities and regulated entities in the private sector, which is the area in which civil penalties have come to play an important role.

6.32 The ALRC has considered the existing civil penalty provisions and whether an alternative approach might have been adopted. There is an argument, for example, that where a person discloses information that is critical to the protection of a matter of national environmental significance—contrary to an express direction of the Minister under s 170B of the *Environment Protection and Biodiversity Conservation Act*—that criminal penalties should apply. The intentional disclosure of information that has been expressly identified as potentially damaging to an important public interest, may well justify criminal penalties.

6.33 The civil penalty provisions in the *Workplace Relations Act*, discussed above, are directed at members of employer and employee associations,<sup>42</sup> and persons providing dispute resolution services as an alternative to the services provided by the AIRC,<sup>43</sup> respectively.

6.34 In relation to persons providing alternative dispute resolution services, it may have been possible to impose contractual secrecy obligations, or criminal penalties. Where the AIRC conducts the dispute resolution itself, s 712 of the Act creates a duty not to disclose information given to the AIRC in the course of the dispute resolution process. This duty would attract the criminal penalties imposed by s 70 of the *Crimes Act*. In this sense there is a lack of consistency between the penalties imposed on the AIRC and its staff and the penalties imposed on external providers of dispute resolution services.

---

40 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

41 See Appendix 4.

42 *Workplace Relations Act 1996* (Cth) sch 1 s 276.

43 Ibid s 715.

6.35 In relation to members of employer and employee organisations, there is no possibility of contractual secrecy obligations. It would have been possible to impose criminal sanctions for unauthorised disclosure, but a choice was made to create a civil penalty provision, perhaps because of the regulatory nature of the relationship between the AIRC and the relevant organisations. In granting an order to allow a member to inspect the financial records of their organisation, the AIRC may make ancillary orders, including an order limiting the use that the person may make of information obtained during the inspection. Breach of such an order also attracts civil penalties.

6.36 In this Discussion Paper, the ALRC is not making any proposals that would give civil penalties a greater role in relation to the protection of Commonwealth information. However, in Chapter 14, the ALRC asks whether there is a gap that needs to be addressed in terms of protecting Commonwealth information where that information is in the hands of persons who are not public sector employees or Commonwealth contractors. It is possible that civil penalties would have a role in this context.

6.37 In addition, in Chapter 9, the ALRC proposes that the courts be given an express power to issue injunctions to restrain a breach of the proposed general secrecy offence or the on-disclosure of information in breach of the proposed subsequent disclosure offence. This proposal recognises that preventing the disclosure of sensitive Commonwealth information is preferable to imposing sanctions once disclosure has occurred.

### Criminal penalties

6.38 In the report, *Same Crime, Same Time: Sentencing of Federal Offenders*, the ALRC identified the purposes for imposing criminal penalties as being to:

- ensure that the offender is justly punished for the misconduct;
- deter the offender and others from committing the same or similar misconduct;
- promote the rehabilitation of the offender;
- protect the community by limiting the capacity of the offender to re-offend;
- denounce the conduct of the offender; and
- promote the restoration of relations between the community, the offender and the victim.<sup>44</sup>

---

<sup>44</sup> Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006). The ALRC recommended that federal sentencing legislation should provide that a court can only impose a sentence on a federal offender for one or more of the abovementioned purposes: Rec 4–1.

6.39 The role of the deterrent effect of criminal penalties has been discussed in a number of other reviews of secrecy laws including, for example, the Treasury *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions*.<sup>45</sup> In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs stated that:

If a penalty is adequate, then it may act as a deterrent to the commission of a crime. Indeed it has been suggested that the worth of the secrecy provisions in the *Crimes Act* is measured by governments not in the number of prosecutions, which are few, but in their deterrence value. However, while prosecutions under the *Crimes Act* are few, this may not indicate the adequacy of the penalty in deterring potential offenders, but rather may be illustrative of the small number of people actually apprehended for those particular offences.<sup>46</sup>

6.40 A number of submissions to this Inquiry also emphasised the importance of the deterrent value of criminal penalties.<sup>47</sup> In considering whether a criminal penalty is appropriate in relation to particular conduct, regard must be had to a number of factors, including: the effect of a criminal conviction; the need for clarity and certainty in describing conduct to which criminal penalties apply; and the public interest in limiting the application of the criminal law to conduct that is deserving of such treatment. Each of these will be considered in turn.

### ***Effect of conviction***

6.41 The AGD *Guide to Framing Commonwealth Offences* states that ‘perhaps the most important factor to be considered in determining whether a provision should be criminal or civil is the effect of a criminal conviction’.<sup>48</sup>

6.42 A conviction is a judicial act that alters an offender’s legal status.<sup>49</sup> A criminal conviction carries a social stigma. This can result in an offender being discriminated against on the basis of his or her criminal record, long after a sentence has been completed.<sup>50</sup> A conviction has many consequences beyond the immediate penalty imposed. A person who is convicted of certain offences may be:

45 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 15.

46 Australian Parliament—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), [5.5.2].

47 Liberty Victoria, *Submission SR 19*, 18 February 2009; Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009; J Renwick, *Submission SR 02*, 11 December 2008.

48 Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 11.

49 R Fox and A Freiberg, ‘Sentences Without Conviction: From Status to Contract in Sentencing’ (1989) 13 *Criminal Law Journal* 297, 300.

50 For example, Human Rights and Equal Opportunity Commission, *Discrimination in Employment on the Basis of Criminal Record—Discussion Paper* (2004).

- ineligible to hold public office;<sup>51</sup>
- ineligible to manage a corporation,<sup>52</sup> or be a director or principal executive officer of a company,<sup>53</sup>
- required to disclose the fact of his or her criminal conviction in a number of circumstances, for example, in obtaining a driver's licence or in seeking employment in certain positions,<sup>54</sup> and
- deported, if he or she is a non-citizen.<sup>55</sup>

6.43 A convicted offender may lose or be unable to continue in, or obtain, suitable employment—for example, he or she may face deregistration from a professional body. For a public sector officer or employee, a conviction for an offence involving the unauthorised disclosure of Commonwealth information is likely to result in adverse career prospects or loss of employment, as well as significant reputational damage.

6.44 A federal offender may also be subject to orders for the confiscation of property in relation to the offence. If a person unlawfully sold Commonwealth information, for example, the proceeds of that sale would be subject to the *Proceeds of Crime Act 2002* (Cth), which establishes a scheme to trace, restrain and confiscate the proceeds of crime committed against federal law.

#### ***Need for clarity and certainty***

6.45 Given the serious consequences of a criminal conviction, it is important that the parameters of conduct that will attract criminal penalties are certain. As a general principle, a person should not be subject to criminal penalties where the scope of the offence is ambiguous.

6.46 Chapter 5 discusses the parameters of the offence created by s 70 of the *Crimes Act*. Under that provision, a current or former Commonwealth officer who discloses information acquired by virtue of his or her position as a Commonwealth officer, being information which it is his or her duty not to disclose, is guilty of an offence punishable by two years imprisonment. The duty not to disclose information is not found in s 70 itself, but may be found most commonly in other specific legislative provisions giving rise to a duty not to disclose official information. Other possible sources of the duty include an employee's common law duty to serve his or her employer with loyalty and fidelity; the equitable duty of confidence of employees to

---

51 For example, a person who has been convicted for any offence punishable by imprisonment for one year or longer cannot be chosen, or sit, as a Senator or a member of the House of the Representatives: *Australian Constitution* s 44(ii).

52 *Corporations Act 2001* (Cth) s 206B.

53 For example, *Life Insurance Act 1995* (Cth) s 245.

54 This is subject to the spent conviction provisions in *Crimes Act 1914* (Cth) pt VIIIC.

55 *Migration Act 1958* (Cth) s 201.

protect the confidential information of their employer; and the terms and conditions of a contract of employment.<sup>56</sup>

6.47 In his report on *Integrity In Government, Official Information*, Paul Finn expressed the view that Commonwealth criminal legislation

simply attaches criminal sanctions to the breach of whatever secrecy obligation happens to bind a given public official. This, of itself, gives reason for pause. But what makes it particularly obnoxious is that ... the secrecy obligations imposed by public service legislation are so all encompassing and unreasonable in their information coverage that strict compliance with them is practically impossible. In their current form those obligations have no place in a modern democratic State. There is an urgent need for their recasting. There is a like need to reconsider what their appropriate relationship should be to the criminal law even after that recasting.<sup>57</sup>

6.48 John McGinness has noted that many secrecy provisions expose public sector officers and employees to criminal sanctions for disclosing information, no matter how innocuous, or for disclosing information that already may be in the public domain.<sup>58</sup>

The fact that a prosecution is unlikely to be initiated for disclosure of non-sensitive information is no answer. A person's potential liability to prosecution should be precisely stated in legislation, not left as a matter of discretion to prosecuting authorities. Uncertainty in operation, as the Franks Committee observed, is one of the major faults of official secrets legislation: 'people are not sure what it means or how it operates in practice or what kinds of action involve a real risk of prosecution'.<sup>59</sup>

### ***Which factors should determine whether criminal penalties apply?***

6.49 A number of commentators and reports have considered the circumstances in which it is appropriate for criminal penalties to apply in relation to the disclosure of Commonwealth information. The views expressed focus on varying factors, including: the nature of the information; the intent of the individual disclosing the information; and the effect on the public interest if the information were to be disclosed.

6.50 McGinness has questioned the need for criminal penalties to protect much of the information currently covered by secrecy provisions. He has suggested that a large number of secrecy provisions could be repealed, and reliance placed on other means of protecting Commonwealth information

such as ... the loyalty of officials, formal and informal sanctions within a career service and between ministerial colleagues, formal public service disciplinary procedures, security checks and training of staff, security classification and privacy

<sup>56</sup> Section 70 and the need to establish a 'duty not to disclose' is described in more detail in Ch 5 and considered further in Ch 7. Section 70 is set out in full in Appendix 5.

<sup>57</sup> P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 43–44.

<sup>58</sup> J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 72.

<sup>59</sup> Ibid, 73 citing Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972).

markings on documents, other physical security measures, Cabinet procedures, the law on official corruption, common law and statutory protection of rights with respect to information (breach of confidence, contract, defamation, copyright, *Privacy Act 1988*).<sup>60</sup>

6.51 The *Review of the Commonwealth Criminal Law*, chaired by Sir Harry Gibbs (the Gibbs Committee), recommended in 1991 that the criminal law should only apply to the unauthorised disclosure of a discrete number of categories of information, ‘no more widely stated than is required for the effective functioning of Government’.<sup>61</sup>

6.52 In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs noted that:

It was generally agreed that the unauthorised disclosure and procurement of confidential third party information is an appropriate matter for the criminal law in some circumstances. Criminal sanctions were considered particularly appropriate where information is deliberately released for profit, or with malicious intent, or possibly where the disclosure is made recklessly.

However, the criminal law should not operate more widely than is needed and it should not be invoked unless there is a specific reason for giving certain information special protection. The reason for restricting the application of the criminal law is that the imposition of criminal sanctions can have serious repercussions and may involve deprivation of an individual’s liberty. Consequently, penal sanctions should be reserved for serious offences where the public interest is best served by imposing those sanctions on the offender.<sup>62</sup>

### ***Submissions and consultations***

6.53 Most stakeholders noted the important role that criminal penalties play in protecting Commonwealth information both as a deterrent, and as an assurance to the Australian community that information provided to the Australian Government is adequately protected. The AGD submitted that, while administrative penalties may be appropriate in dealing with less serious cases, criminal penalties are necessary where a Commonwealth officer is in serious breach of the public trust and confidence placed in him or her by the community:

A criminal offence is the ultimate sanction for breaching the law. Criminal offences should be used where the relevant conduct involves considerable harm to society, the environment or Australia’s national interests, including security interests.<sup>63</sup>

---

60 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 76.  
61 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 330.

The categories of information the subject of the Gibbs Committee’s recommendation are discussed below.

62 Australian Parliament—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), [7.2.7]–[7.2.8].

63 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

6.54 The Australian Intelligence Community noted that, particularly in the intelligence context, the unauthorised disclosure of Commonwealth information can have very serious consequences and should remain subject to criminal penalties.<sup>64</sup>

6.55 APRA noted that the deterrent value of criminal penalties is important where there is much to gain by disclosing commercial information.<sup>65</sup> The Australian Commission for Law Enforcement Integrity also commented on the importance of the deterrence value of criminal penalties.<sup>66</sup> The Australian Securities and Investments Commission (ASIC) submitted that the critical factor in determining when criminal penalties should apply is the intention of the accused: ‘There is a stronger argument for criminal culpability if the offender deliberately discloses information for profit or with malicious intent’.<sup>67</sup> ASIC also noted that:

Caution should be exercised in attempting to create a strict divide between conduct that attracts only administrative penalties and conduct that gives rise to other penalties. Doing so would render the secrecy provisions inflexible so that they may not provide a remedy that is most appropriate for the particular circumstances of each breach.<sup>68</sup>

6.56 The Department of Human Services (DHS) noted that portfolio agencies collect and generate a wide range of sensitive information about individuals including: income and employment information (Centrelink); family relationship and responsibility information (Child Support Agency); details of healthcare, medication and hospital treatment received (Medicare Australia); and information about disabilities or injuries (CRS Australia, Australian Hearing, Centrelink); as well as competitive commercial information about businesses (such as the viability of a business, client lists and business plans). In such circumstances, the DHS noted that:

The ability to point to an offence provision protecting that information gives assurance to customers, as well as enhancing the agencies’ credibility as to the seriousness with which they protect customer information.<sup>69</sup>

6.57 The Department of Education, Employment and Workplace Relations recognised that significant harm can be caused to individuals or the Commonwealth by the unauthorised disclosure of Commonwealth information and submitted that:

there is a recognised need for there to be consequences flowing from such inappropriate action. The *Privacy Act 1988* by itself, however, only partly serves as a useful deterrent, given that it regulates the actions of an agency rather than the

---

<sup>64</sup> Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

<sup>65</sup> Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

<sup>66</sup> Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

<sup>67</sup> Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

<sup>68</sup> *Ibid.*

<sup>69</sup> Department of Human Services, *Submission SR 26*, 20 February 2009.

offending individual. In this sense, having a criminal offence provision which attaches to the unauthorised handling of information has value in being a useful deterrent.<sup>70</sup>

6.58 Other stakeholders noted that criminal penalties should only be used when strictly required for the effective functioning of government.<sup>71</sup> Liberty Victoria cautioned that:

care must be taken when framing criminal offences to ensure that the provisions only penalise intentional (or reckless) behaviour in specific situations. While criminal sanctions may be appropriate in punishing misuse of the most secret information, administrative penalties should be considered more appropriate in the handling of less secret information, where there exists no intention or reckless fault element.<sup>72</sup>

6.59 PIAC expressed the view that, subject to the availability of injunctions to restrain disclosure, the law of breach of confidence was sufficient to protect all but the most sensitive Commonwealth information:

Given the legitimate interest of electors in the activities of government and its emanations, it is hard to see why disclosure by a Commonwealth public servant of Commonwealth information having no inherent quality of confidence should be a criminal offence.

Unauthorised disclosure of highly confidential non-government information by private individuals gives rise (absent an element of personal dishonesty, as in fraud, insider trading and the like) to civil liability only. Disclosure by a government employee of innocuous government information can currently give rise to criminal liability. PIAC believes that the current review provides a valuable opportunity to remedy this anomaly.<sup>73</sup>

6.60 Ron Fraser submitted that:

I doubt very much whether it is necessary in day-to-day situations for officers to be subject to criminal penalties in order for them to perform their duties with a strong ethic of confidentiality. While some penalties are needed in addition to systemic reinforcement, they don't need to be criminal in nature except in the most serious cases.<sup>74</sup>

#### *ALRC's views*

6.61 The ALRC agrees that, consistent with the ‘enforcement pyramid’ model, criminal penalties for disclosure of Commonwealth information ‘should be reserved for serious offences where the public interest is best served by imposing those sanctions on the offender’.<sup>75</sup> It seems clear, however, that there is a role for the criminal law in

---

70 Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

71 Law Council of Australia, *Submission SR 30*, 27 February 2009.

72 Liberty Victoria, *Submission SR 19*, 18 February 2009.

73 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

74 R Fraser, *Submission SR 42*, 23 March 2009.

75 Australian Parliament—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), [7.2.8].

certain circumstances. Commonwealth information includes a range of highly sensitive information such as national security information, information relating to defence, valuable commercial information and sensitive personal information. Unauthorised disclosure of this kind of information has the capacity to cause real harm to important public interests, and to the effective functioning of government.

6.62 The role of the criminal law in publicly punishing, deterring, and denouncing offending behaviour is appropriate when applied to behaviour that harms, is reasonably likely to harm or intended to harm important public interests. Given the adverse consequences of a criminal conviction, however, it is the ALRC's view that it is inappropriate to apply such penalties to disclosures that were not intended and are unlikely to cause such harm.

6.63 As noted by McGinness, above, there is a variety of other mechanisms in place to protect Commonwealth information, including administrative sanctions, contractual obligations and the general law. In these circumstances, the breadth of some existing provisions, such as ss 70 and 79(3) of the *Crimes Act*, does not appear to be justified. These provisions create criminal offences for the disclosure of Commonwealth information without any express or implied requirement that the disclosure was harmful or was intended to be harmful in any way. In the ALRC's view, this kind of blanket provision potentially imposes criminal liability in circumstances that do not merit such a response. This is inconsistent with the 'enforcement pyramid' model.

6.64 The ALRC proposes a new general secrecy offence that is more limited than the current *Crimes Act* provisions and requires that the unauthorised disclosure involve some harm, a reasonable likelihood of harm, or an intention to harm specified public interests.<sup>76</sup> This proposed new offence, discussed in detail below and in the following chapters, is intended to ensure that criminal liability is only imposed where there is a level of culpability that would justify the imposition of criminal penalties and all the consequences that a criminal conviction entails.

6.65 The ALRC is not suggesting, however, that this general secrecy offence replace all existing secrecy offences. Chapters 10 to 12 consider the circumstances in which more specific secrecy provisions imposing criminal sanctions remain justified. In Chapter 10, the ALRC proposes that any specific secrecy offence should generally require that the unauthorised disclosure involve a reasonable likelihood of harm to specified public interests.<sup>77</sup> The ALRC also examines the possibility that, in relation to some information—such as national security classified information—the way in which specific secrecy offences are framed, and the context in which they operate, provide a

---

76 Consistent with Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

77 Proposal 10–1.

sufficient likelihood that harm will be caused by an unauthorised disclosure and that, therefore, an express requirement of harm is unnecessary.<sup>78</sup>

### **The need for a general secrecy offence**

6.66 There are two general criminal offence provisions in the *Crimes Act* that deal with the unauthorised disclosure of Commonwealth information. Section 70 deals with the disclosure of information by Commonwealth officers in breach of a duty not to disclose, while s 79 deals with the disclosure of ‘prescribed information’ by any person with a duty to keep it secret.<sup>79</sup>

6.67 Although s 79 is generally concerned with espionage activity, s 79(3) is drawn very widely and prohibits the unauthorised communication of ‘prescribed information’—which is defined, in part, as information made or obtained by a person owing to his or her position as a current or former Commonwealth officer, office holder or government contractor that, by reason of its nature or the circumstances under which the information was made or obtained, or for any other reason, it is his or her duty to treat as secret.

6.68 As noted by the Gibbs Committee, the combined effect of these provisions is that ‘the unauthorised disclosure of most information held by the Commonwealth Government and its agencies is subject to the sanctions of the criminal law’.<sup>80</sup>

6.69 In relation to general offences, the *Guide to Framing Commonwealth Offences* states that:

Broadly framed provisions of general application were placed in the *Criminal Code* to avoid the technical distinctions, loopholes, additional prosecution difficulty and appearance of incoherence associated with having numerous slightly different provisions to similar effect across Commonwealth law. There are also some provisions concerning offences in the *Crimes Act*. It is intended that these will be transferred to the *Criminal Code* in due course.

Where a relevant *Criminal Code* or *Crimes Act* provision applies, separate provision should not be made in another Act.<sup>81</sup>

6.70 Chapters 10 to 12 consider the plethora of specific secrecy offences in Commonwealth legislation and make a number of proposals intended to ensure greater coherence and consistency across such provisions, where they are retained. This is particularly important because, in some circumstances, the unauthorised disclosure of Commonwealth information may amount to an offence under a general secrecy

78 Question 10–1.

79 These provisions are described in detail in Ch 5 and set out in full in Appendix 5.

80 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [35.12].

81 Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 16.

provision in the *Crimes Act* as well as an offence under a more specific secrecy provision in another piece of Commonwealth legislation. In these situations, an alleged offender can be prosecuted under either law.<sup>82</sup>

6.71 When determining the charges to be laid or proceeded with, the Commonwealth Director of Public Prosecution's *Prosecution Policy of the Commonwealth* states that the provisions of a specific Act should be relied upon rather than the general provisions of the *Crimes Act*, unless to do so 'would not adequately reflect the nature of the criminal conduct disclosed by the evidence'.<sup>83</sup> The proposals in Chapter 12 aim to ensure that specific secrecy provisions are only enacted or retained where the context or circumstances require that elements of the offence—for example, the parties covered—are significantly different from those in the general offence.

6.72 As discussed in Chapter 5, there have been a small number of prosecutions for breach of ss 70 and 79(3). In 1990, McGinness noted that prosecutions under these provisions have been rare and 'have not had the political overtones that prosecutions in other countries have had'.<sup>84</sup> He suggested that because the provisions have not been subject to the same level of controversy as equivalent provisions in other countries, this might explain, in part, why the provisions have not been substantially amended since the 1960s. McGinness expressed the view that these general secrecy provisions need to be replaced by specific provisions that 'introduce certainty and consistency to the regulation of unauthorised public disclosure'.<sup>85</sup>

6.73 The Gibbs Committee recommended that the 'catch-all' provisions of ss 70 and 79(3) of the *Crimes Act* be repealed and replaced with provisions that impose criminal sanctions for the disclosure of certain types of information. As noted in Chapter 2, the Gibbs Committee recommended that these types of information include:

- information relating to intelligence and security services, defence and foreign relations;
- information obtained in confidence from, or entrusted in confidence to, other governments or international organisations;
- information the disclosure of which would be likely to result in the commission of an offence; facilitate an escape from legal custody or the doing of an act prejudicial to the safekeeping of persons in legal custody; or impede the

---

82 *Crimes Act 1914* (Cth) s 4C.

83 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <[www.cdpp.gov.au/Publications/ProsecutionPolicy/](http://www.cdpp.gov.au/Publications/ProsecutionPolicy/)> at 26 August 2008, [2.22].

84 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 71.

85 *Ibid*, 76.

prevention or detection of offences or the apprehension or prosecution of suspected offenders.<sup>86</sup>

6.74 The Gibbs Committee concluded that it was also necessary to prove that the disclosure caused damage in certain circumstances. The Gibbs Committee's recommendations are discussed further in Chapter 7.

6.75 In IP 34, the ALRC asked whether the handling of Commonwealth information should remain subject to a general secrecy offence and, if so, whether an updated offence should be included in the *Criminal Code*.<sup>87</sup> The Australian Government intends the *Criminal Code* to be the principal piece of federal legislation containing serious criminal offences and that substantive criminal provisions in other, older pieces of law, such as the *Crimes Act*, be progressively reviewed, and either 'modernised' and 'migrated' to the *Criminal Code*, or repealed. Ultimately, the intention is that the *Crimes Act* will deal only with police powers (such as arrest, detention, and search and seizure) and criminal procedure.<sup>88</sup>

### ***Submissions and consultations***

6.76 Most submissions expressed support for retaining a general secrecy offence. The AGD submitted that:

it would seem desirable to retain a general offence of non-disclosure. There is a strong argument for consideration to be given to updating the offence currently in section 70 of the *Crimes Act 1914*, given that it has existed in its current form since 1960, which pre-dates the introduction of the FOI Act and other new administrative law mechanisms. ...

Updating the section 70 general offence to clarify and better target its scope of operation could result in greater reliance on the general offence, and consequently, fewer secrecy provisions being inserted in various Commonwealth Acts. It would be consistent with current policy to place any general offence in the *Criminal Code* rather than in the *Crimes Act*.<sup>89</sup>

6.77 The ATO, the Australian Federal Police and other stakeholders also expressed support for a general criminal offence in order to cover information not covered by specific secrecy provisions.<sup>90</sup> APRA noted that it was important to have both a specific secrecy provision, such as s 56 of the *Australian Prudential Regulation Authority Act 1998* (Cth)—covering information and documents relating to regulated entities—as well as a general offence, such as s 70 of the *Crimes Act*, to cover unauthorised

---

86 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.50].

87 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 2–1.

88 The development of the *Criminal Code* was considered in detail in Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Ch 1.

89 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

90 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Australian Federal Police, *Submission SR 33*, 3 March 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009.

disclosure of information that is not protected by s 56, for example, information about confidential new policy proposals.<sup>91</sup>

6.78 The DHS suggested that a general secrecy offence would also address other gaps in the regulatory regime:

Other legislative regimes for dealing with sensitive information contain gaps in coverage. For example, the *Privacy Act* does not cover information about deceased individuals or about entities which are not individuals (corporations, states, trusts etc); the *Public Service Act* does not regulate former employees or [contracted service providers] and their staff; the equitable doctrine on the obligation not to breach confidence is quite technical and often difficult to make out; confidentiality deeds usually do not address all aspects of dealing with protected information such as collection and solicitation or subsequent dealings where information was obtained through an unauthorised disclosure. Coverage of these areas is considered important for the overall management of sensitive information in the Commonwealth's possession, and secrecy laws play an important role.<sup>92</sup>

6.79 In addition, ASIC noted that a general criminal offence helps to ensure ‘parity of treatment of those disclosures that are regarded as properly attracting criminal penalties’.<sup>93</sup>

6.80 In contrast, and as noted above, PIAC submitted that s 70 of the *Crimes Act* should be repealed and not replaced and greater reliance placed on the equitable duty of confidence.<sup>94</sup> The NSW Young Lawyers also suggested that repealing s 70 and placing reliance on portfolio specific legislation was an option that should be considered.<sup>95</sup>

#### ***ALRC’s views***

6.81 The ALRC considers that there is a need for a general secrecy offence, to be included in the *Criminal Code*, for a number of reasons. A new general secrecy offence would set a benchmark for the imposition of criminal penalties for the unauthorised disclosure of Commonwealth information. Any specific provision that differed in significant respects from the general provision—for example, in the penalty imposed—would require justification. In addition, a well drafted, clear and principled general secrecy offence should reduce the need for the existing plethora of specific offences. This would be consistent with the AGD *Guide to Framing Commonwealth Offences* and with the ALRC’s proposals in Chapters 10 to 12.

---

91 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

92 Department of Human Services, *Submission SR 26*, 20 February 2009.

93 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

94 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

95 NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009.

6.82 The general offence would cover a number of gaps left by the administrative secrecy provisions, including former Commonwealth officers, and by more specific secrecy provisions that focus, for example, on a particular function of an agency or on particular information held by an agency.

6.83 In Chapters 7, 8 and 9, the ALRC considers the elements of the proposed offence in detail, including whose conduct should be regulated and the relevant physical and fault elements to be included. The ALRC concludes that the proposed general secrecy offence should regulate disclosure of Commonwealth information by ‘Commonwealth officers’, defined to include all those who work in the executive branch of government, as well as those who provide services under contract to or on behalf of the Australian Government.

6.84 The most significant change proposed is that under the new offence provision, the prosecution should be required to prove that a particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to a specified public interest. This approach is intended to balance the need to protect certain Commonwealth information with the public interest in an open and accountable system of government. In finding this balance, the ALRC was drawn to the idea that the general secrecy offence should complement the *Freedom of Information Act 1982* (Cth) (the FOI Act).

6.85 The objects of the FOI Act expressly include extending ‘as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth’. This right is limited by certain exceptions and exemptions considered ‘necessary for the protection of essential public interests and the private and business affairs of persons’.<sup>96</sup> In Chapter 7, the ALRC considers each of the FOI exemptions in detail, and suggests that a subset of the public interests protected by the FOI exemptions should form the basis of the general secrecy offence. The ALRC has identified those public interests—such as the protection of national security, defence and international relations; and the enforcement of the criminal law—where the potential for harm is of such a serious nature as to warrant the imposition of criminal sanctions.

6.86 As noted above, in proposing a general secrecy offence, the ALRC is not suggesting that this should be the only criminal offence provision regulating the disclosure of Commonwealth information. The general secrecy offence is intended to serve as an umbrella offence applying to all current and former Commonwealth officers. In Chapters 10 to 12, the ALRC considers the circumstances in which more specific secrecy offences are still warranted, for example, where the circumstances dictate the need for a different level of regulation.

---

96        *Freedom of Information Act 1982* (Cth) s 3.

**Proposal 6–1** Sections 70 and 79(3) of the *Crimes Act 1914* (Cth) should be repealed and replaced by a new offence in the *Criminal Code* (Cth), which regulates the disclosure of Commonwealth information by Commonwealth officers (the ‘general secrecy offence’).



## 7. General Secrecy Offence: Harm to Public Interests

---

### Contents

Introduction	223
Duty not to disclose information	224
Submissions and consultations	226
ALRC's views	227
Harm to identified public interests	228
Submissions and consultations	231
ALRC's views	236
Fault element attaching to harm	250

### Introduction

7.1 As discussed in Chapter 6, the ALRC is proposing that ss 70 and 79(3) of the *Crimes Act 1914* (Cth) be repealed and that there should be a new general secrecy offence created and located in the *Criminal Code* (Cth).<sup>1</sup> In the Issues Paper, *Review of Secrecy Laws* (IP 34),<sup>2</sup> the ALRC sought stakeholder views on how such an offence should be framed.<sup>3</sup>

7.2 In this chapter, the ALRC proposes to considerably narrow the scope of the general secrecy offence in comparison with the existing provisions. This approach is intended to reflect the trend towards open government, articulated clearly in the objects clause proposed in the Exposure Draft Freedom of Information Amendment (Reform) Bill 2009 (the FOI Exposure Draft Bill). The FOI Exposure Draft Bill indicates that the objects of the FOI Act should be to promote Australia's representative democracy by increasing public participation in Government processes; by increasing scrutiny, discussion, comment and review of the Government's activities; and to increase recognition that information held by the Government is to be managed for public purposes, and is a national resource.<sup>4</sup>

---

<sup>1</sup> Sections 70 and 79(3) are described in detail in Chs 5 and 6, and set out in full in Appendix 5.

<sup>2</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

<sup>3</sup> Ibid, Question 2–2.

<sup>4</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, cl 3.

7.3 Consistently with this approach to Commonwealth information, the ALRC proposes that a disclosure should only attract criminal penalties under the general secrecy offence where the prosecution can prove that the particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to specified public interests, such as the security or defence of the Commonwealth. This is consistent with the ‘enforcement pyramid’ model discussed in Chapter 6, in that criminal penalties are reserved for the most serious circumstances. In the absence of any likely, intended or actual harm to those public interests, the ALRC is of the view that unauthorised disclosure of Commonwealth information should be dealt with by the imposition of administrative penalties or the pursuit of contractual or general law remedies.<sup>5</sup>

7.4 Chapter 8 goes on to consider other elements of the offence, including what and whose conduct should be regulated. Chapter 9 deals with what exceptions and defences should be available under the proposed general secrecy offence, and what penalties should apply for breach of the offence.

### **Duty not to disclose information**

7.5 In considering how a new general secrecy offence should be framed, the ALRC examined a range of existing provisions—in particular ss 70 and 79(3) of the *Crimes Act*—including those aspects of existing provisions that have drawn consistent criticism. One aspect that has attracted adverse attention is the lack of clarity and certainty around when a ‘duty not to disclose information’ might arise under s 70.

7.6 Section 70 provides that it is an offence for a Commonwealth officer to disclose information ‘which it is his or her duty not to disclose’. As noted in Chapter 6, this duty is not found in s 70 itself, but must be found elsewhere. Most commonly, the source of the duty is a specific legislative provision giving rise to a duty not to disclose official information.<sup>6</sup>

7.7 For example, s 13 of the *Public Service Act 1999* (Cth), which sets out the Australian Public Service (APS) Code of Conduct, provides that an APS employee must comply with any conduct requirement prescribed by the regulations.<sup>7</sup> Regulation 2.1(3) of the *Public Service Regulations 1999* (Cth) sets out a duty not to disclose information:

an APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee’s employment if it is reasonably

---

5 Administrative penalties and contractual remedies are considered in Chs 13 and 14. General law remedies are considered in Ch 5.

6 See, eg, *R v Goreng Goreng* [2008] ACTSC 74, [8]; *Johnston v Director of Public Prosecutions (Cth)* (1989) 90 ACTR 7, 9–10.

7 *Public Service Act 1999* (Cth) s 13(13).

foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.<sup>8</sup>

7.8 Regulation 2.1 provides an example of a provision that sets out a duty of non-disclosure and makes express reference to the application of s 70 of the *Crimes Act* in an accompanying note:

*Note:* Under section 70 of the *Crimes Act 1914*, it is an offence for an APS employee to publish or communicate any fact or document which comes to the employee's knowledge, or into the employee's possession, by virtue of being a Commonwealth officer, and which it is the employee's duty not to disclose.

7.9 Other secrecy provisions are not expressly linked to s 70 in this way. For example, s 114(1) of the *Food Standards Australia New Zealand Act 1991* (Cth) states that:

It is the duty of a person who is a member of the Board, a member of the staff of the Authority, a member of a committee or a person engaged as a consultant under section 136 not to disclose any confidential commercial information in respect of food that has been acquired by the person because of being such a member or consultant.

7.10 The provision does not specify a penalty for breach and makes no reference to the *Crimes Act*. Presumably, s 70 applies but its application is not readily apparent.<sup>9</sup>

7.11 A duty may also arise from other sources, such as an employee's general law duties<sup>10</sup> or, possibly, the terms and conditions of an employment contract. As discussed in Chapter 5, there is some doubt about whether the 'duty' in s 70 can arise from a contractual term, but it seems clear that it must be a legal—as opposed to a moral—duty.<sup>11</sup> The lack of clarity as to what duties may give rise to criminal liability under s 70 led McGinness to observe that:

The obscure nature of the duties was the subject of criticism when the *Crimes Act* was first enacted and has been put forward by prosecuting authorities as one reason for their failure to prosecute possible breaches.<sup>12</sup>

7.12 In IP 34, the ALRC asked whether it was appropriate for a general secrecy offence to rely on a duty arising separately under the general law or under other legislative provisions.<sup>13</sup>

---

8 The full text of reg 2.1 of the *Public Service Regulations* is set out in Appendix 5.

9 The provision does, however, specify a maximum penalty of two years imprisonment in circumstances where an unauthorised subsequent disclosure occurs: *Food Standards Australia New Zealand Act 1991* (Cth) s 114(8). A similar approach is taken in *Australian Hearing Services Act 1991* (Cth) s 67.

10 The common law duty of loyalty and fidelity and the equitable duty of confidence are considered in Ch 5.  
11 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 258–259.

12 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 73.  
13 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 2–2.

## **Submissions and consultations**

7.13 The Australian Government Attorney-General's Department (AGD) submitted that:

It would seem preferable for a general secrecy offence to set out the circumstances when a duty of non-disclosure might arise, as this would provide greater clarity and certainty to Commonwealth officers and others. It would also tend to reduce the perceived need for including specific secrecy laws in other legislation on the basis that it is not sufficiently clear whether the general offence would apply, or to create a specific duty for the purpose of the general offence. However, it is unlikely to be possible to set out exhaustively all the circumstances that may give rise to a non-disclosure duty. Therefore, it seems advisable to retain a level of flexibility in the general offence to allow for non-disclosure duties to arise elsewhere, such as in other legislation, pursuant to contractual agreements or at common law.<sup>14</sup>

7.14 Noting that it would not be appropriate to include an offence in one piece of legislation and the penalty in another, the AGD submitted that it may, however, be appropriate to include a legislative note referring to the existence of an offence and penalty in another piece of legislation.<sup>15</sup> The Treasury agreed that provisions containing a duty of non-disclosure, which do not themselves create an offence, should at least cross-refer to the section that establishes the offence and the penalty.<sup>16</sup>

7.15 Other stakeholders expressed a level of concern that the duty not to disclose should be found separately from the provision imposing the criminal sanction.<sup>17</sup> The Community and Public Sector Union (CPSU) expressed particular concern about the relationship between reg 2.1 of the *Public Service Regulations* and s 70 of the *Crimes Act*. The CPSU submitted that only disclosure of classified or secret Commonwealth information should be subject to criminal penalties. Disclosure of other confidential information should be dealt with on an administrative level—as a breach of the APS Code of Conduct in the *Public Service Act*—in the same way as other employment-related disciplinary matters.<sup>18</sup>

7.16 Ron Fraser agreed, stating that:

So long as s 70 continues to penalise breaches of duty to be found in other legislation, breaches of Public Service Regulation 2.1 will be subject both to administrative penalties and to possible prosecution under s 70. It is preferable for it to be restricted to the former.<sup>19</sup>

---

14 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

15 Ibid.

16 The Treasury, *Submission SR 22*, 19 February 2009.

17 See, eg, Law Council of Australia, *Submission SR 30*, 27 February 2009.

18 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

19 R Fraser, *Submission SR 42*, 23 March 2009.

7.17 The Public Interest Advocacy Centre (PIAC) submitted that:

Any criminal secrecy provision of general application should not be triggered by breach of an obligation arising under the general law, but upon breach of a clearly identified duty of non-disclosure, set out in the relevant statute. ...

All secrecy provisions should make clear on their face the consequences of breach. If the consequences of breach are contained in another piece of legislation, the secrecy provision should cross-reference it, although this is not the preferred approach.<sup>20</sup>

### ALRC's views

7.18 In Chapter 6, the ALRC considers the need for clarity and certainty in the criminal law. It appears that there are real concerns about s 70 of the *Crimes Act* in this regard—in particular, about the need to establish a duty independently of the offence provision—and also about some of the terminology used in s 79(3). Although it is possible, for example, to include a cross-reference to s 70 in a provision giving rise to a duty of non-disclosure, this is not ideal. The ALRC considers that it is preferable for the offence provision itself to set out all the elements of the offence and the penalty attached to the offence. This is consistent with the AGD *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, which states that:

It is normally desirable that the content of an offence be stated in the offence itself, so that the scope and effect of the offence is clear to the Government, the Parliament and those subject to the offence.<sup>21</sup>

7.19 In particular, the ALRC is concerned that, where no cross-reference to s 70 is included in legislation containing a duty of non-disclosure, it is unclear whether the Australian Parliament expressly considered the link with s 70 and the fact that the duty created had the potential to give rise to criminal sanctions.

7.20 The *Guide to Framing Commonwealth Offences* also notes that:

A further problem with such provisions is that they are a form of general offence that applies a single maximum penalty to a wide range of potential conduct of unspecified seriousness.<sup>22</sup>

7.21 This problem clearly arises in relation to s 70. While the offence and maximum penalty are set out in the *Crimes Act*, other elements—such as the scope of the duty imposed and the type of information protected—are set out in other Acts and may vary widely.

---

20 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

21 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 14.

22 Ibid.

7.22 For these reasons, the ALRC proposes a general secrecy offence which does not rely on a duty arising under another Act. Instead, all elements of the offence will be set out in the offence itself. As discussed in the following chapters, the proposed offence will apply to all current and former Commonwealth officers and to any information to which the officer has access by reason of being, or having been, an officer. However, the provision will be limited by the need to establish that a particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to specified public interests.

7.23 This approach gives rise to the need to consider those provisions that currently establish a duty not to disclose Commonwealth information, but do not themselves create a criminal offence.<sup>23</sup> In the ALRC's view, these provisions will need to be reviewed to decide whether they are necessary at all and, if so, whether they should attract administrative or criminal penalties. Chapters 10 to 12 consider when specific secrecy offences should be repealed because they substantially replicate the proposed new general secrecy offence. Where a specific offence can be justified, the chapters provide guidance on how such provisions should be framed in order to be more consistent with the policy underlying the proposed general secrecy offence, and with each other.

7.24 In some cases, it will be appropriate to impose only administrative sanctions for unauthorised disclosure of Commonwealth information. For example, in relation to reg 2.1 of the *Public Service Regulations*, the effect of repealing s 70 will be that breach of the regulation may attract the administrative penalties set out in the *Public Service Act*, but will no longer attract criminal penalties under the *Crimes Act*. In the ALRC's view, this is an acceptable outcome. The ALRC considers that breach of reg 2.1 should be treated in the same way as a breach of any other element of the APS Code of Conduct. Where it is the Australian Parliament's intention to impose criminal penalties for disclosure of Commonwealth information, this should be done expressly in offence provisions so that there is a clear and certain link between the conduct being criminalised and the criminal penalty imposed.

7.25 In the following section, and Chapters 8 and 9, the ALRC considers in detail how the new general secrecy offence should be framed.

## Harm to identified public interests

7.26 In the 2004 report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, the ALRC recommended that a duty of secrecy should only be imposed in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.<sup>24</sup> As discussed in

---

23 These provisions are also discussed in Ch 5.

24 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

Chapter 5, this is the approach the courts have adopted in considering the extent to which government information is protected by the common law duty of loyalty and fidelity or the equitable duty of confidence.

7.27 While the ALRC is proposing to narrow the scope of the new general secrecy offence in comparison with the existing provisions, it is important to ensure that where information is disclosed that does damage, is reasonably likely to damage, or is intended to damage important public interests, there are appropriate criminal provisions in place. In the ALRC's view, this will create a better balance between the need to protect Commonwealth information and the public interest in open and accountable government. In this section, the ALRC considers which public interests require the protection of the criminal law and therefore should be reflected in the proposed general secrecy offence.

7.28 Most existing secrecy provisions do not expressly indicate the public interest they are seeking to protect. For example, s 51(2) of the *Australian Crime Commission Act 2002* (Cth) provides that:

A person to whom this section applies who, either directly or indirectly, except for the purposes of a relevant Act or otherwise in connection with the performance of his or her duties under a relevant Act, and either while he or she is or after he or she ceases to be a person to whom this section applies:

- (a) makes a record of any information; or
- (b) divulges or communicates to any person any information;

being information acquired by him or her by reason of, or in the course of, the performance of his or her duties under this Act, is guilty of an offence punishable on summary conviction by a fine not exceeding 50 penalty units or imprisonment for a period not exceeding 1 year, or both.

7.29 This provision binds the Chief Executive Officer, staff and others associated with the Australian Crime Commission (ACC), and applies to any information acquired in the course of their duties under the Act. It is not necessary to show that the unauthorised conduct—making a record of, divulging or communicating information—would cause, was likely to cause or was intended to cause any harm to any public interest. While these issues might be taken into consideration by the Commonwealth Director of Public Prosecutions (CDPP) in deciding whether to prosecute a person for a breach of the provision, or by the court in deciding on an appropriate penalty for breach of the provision, they do not form an element of the offence itself.

7.30 By way of contrast, a small number of secrecy provisions expressly require that the unauthorised conduct cause, be likely to cause, or be intended to cause, harm to a specific public interest. Some of these provisions are discussed in Chapter 10. An example is s 58 of the *Defence Force Discipline Act 1982* (Cth). The necessary harm to the public interest identified in that provision is that the conduct must be 'likely to be

prejudicial to the security or defence of Australia'. Strict liability applies to this element of the offence and so it is not necessary to establish that the person was reckless or intended to prejudice the security or defence of Australia, just that the disclosure was likely to do so.

7.31 Another example is s 193S(3) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth), which expressly requires—as an element of a number of the offences set out in that section—that the conduct would, or would be likely to, harm specific public interests. The provision makes it an offence for an Indigenous Land Corporation (ILC) officer to disclose information ‘considered sacred or otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders’, where ‘the disclosure would be inconsistent with the views or sensitivities of those Aboriginal persons or Torres Strait Islanders’.

7.32 In its final report, *The Review of the Commonwealth Criminal Law*, the Committee chaired by Sir Harry Gibbs (the Gibbs Committee) considered the need for secrecy offences to include a requirement to prove that the unauthorised disclosure caused some harm and, in this regard, drew a distinction between different categories of protected information. In relation to information relating to defence or foreign relations, for example, the Gibbs Committee stated that:

Obviously, the description of information as relating to defence or foreign relations would be so wide that, unless qualified in some way, they would apply to information of an innocuous nature. Thus, no submission disputed that these descriptions needed to be qualified by a requirement to prove harm.<sup>25</sup>

7.33 The Gibbs Committee recommended that the prosecution should be required to prove harm in the case of a disclosure of information:

- relating to defence or foreign relations; and
- obtained in confidence from foreign governments and international organisations.<sup>26</sup>

7.34 The Gibbs Committee also recommended that, where proof of harm is required, it should be a defence for a person charged with an offence that he or she did not know, and had no reasonable cause to believe, that the information related to the matters in question or that its disclosure would be damaging.<sup>27</sup> However, in some areas, the Committee considered it was appropriate to impose criminal sanctions without having to establish any harm to the public interest—notably in relation to intelligence and national security information.<sup>28</sup>

---

<sup>25</sup> H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 322.

<sup>26</sup> Ibid, 331.

<sup>27</sup> Ibid, 332.

<sup>28</sup> Ibid, 323. See, further, Chs 2 and 10.

7.35 In contrast, McGinness argued that ‘it is not sufficient to point to a category of official information that needs protection from unauthorised disclosure’, commenting that some additional justification should be necessary to attract criminal sanctions.<sup>29</sup>

7.36 In IP 34, the ALRC asked whether all secrecy provisions should expressly require that the unauthorised conduct cause, be likely to cause, or intended to cause harm to a specified public interest.<sup>30</sup>

### Submissions and consultations

7.37 A number of stakeholders expressed concern about the imposition of an express requirement to prove harm in every case. The Australian Taxation Office (ATO) submitted that such a requirement would be inherently uncertain and difficult to apply. In addition, the ATO was of the view that taxpayers would be less likely to provide full and frank information concerning their tax affairs if they were concerned that the ATO could not adequately protect the confidentiality of the information.<sup>31</sup>

7.38 The Treasury was also concerned that an express harm requirement would reduce certainty and clarity. In The Treasury’s view, the relevant public interests should be taken into consideration in developing legislation regulating whether or not information is permitted to be disclosed for a specified purpose.<sup>32</sup>

7.39 The Australian Prudential Regulation Authority (APRA) and the Australian Bureau of Statistics (ABS) suggested that an express harm requirement was not desirable in their own context-specific legislation. In APRA’s view, it is implicit in s 56 of the *Australian Prudential Regulation Authority Act 1998* (Cth) that unauthorised disclosure would harm the public interest.<sup>33</sup> The ABS expressed the view that the absolute nature of the ABS specific provisions was their strength, but noted that some contexts could allow for a public interest element:

The unauthorised disclosure of identifiable information provided for statistical purposes should be subject to criminal penalties. Unauthorised disclosure of other statistical information (eg unauthorised disclosure of aggregated statistical results prior to their official release) should be subject to criminal penalties where such disclosure is detrimental to the public interest.<sup>34</sup>

7.40 The AGD submitted that it should not be necessary to establish proof of harm in relation to some categories of information, such as intelligence information, but that in relation to the general secrecy offence,

29 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 76.

30 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–7.

31 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

32 The Treasury, *Submission SR 22*, 19 February 2009.

33 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

34 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

it may be appropriate to focus upon disclosure of information that could have some specified harm. This would prevent secrecy laws being too broad and taking a ‘blanket’ approach. The public interests that require protection may include things such as the effective working of government, prejudice to national security or defence, international relations, and the effective working of law enforcement agencies.<sup>35</sup>

7.41 The AGD noted that this approach had been taken in reg 2.1 of the *Public Service Regulations*, discussed above. Regulation 2.1 prohibits the disclosure of information ‘if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government’. The AGD suggested that ‘reasonably likely to cause harm’ would be a useful model to adopt in relation to the general secrecy offence as it establishes an objective test. The AGD submitted that a requirement to prove actual harm may create evidential difficulties, ‘particularly when the harm may not necessarily be obvious or easily quantifiable (such as with the disclosure of Cabinet documents)’. The AGD also noted that evidential difficulties can arise in establishing that a person acted with an intention to cause harm:

Requiring proof of such intention in all cases would be too high a threshold and would be likely to reduce the effectiveness and potentially the deterrent effect of secrecy laws. An option that could be considered is having tiered offences, so a higher penalty applies where it can be proved that a person acted with intention to cause harm to the public interest.<sup>36</sup>

7.42 The CDPP was also concerned that a requirement to prove harm to specified public interests would give rise to evidential difficulties.<sup>37</sup>

7.43 The Australian Federal Police (AFP) supported the idea of an offence hierarchy with a basic offence provision of unauthorised disclosure of information, with a lower penalty; and a more serious offence provision requiring the prosecution to prove an intention to harm the public interest, with a higher penalty.<sup>38</sup>

7.44 Other stakeholders, however, expressed strong support for expressly including a requirement of harm to the public interest in any secrecy provision. For example, PIAC submitted that the mere fact that information fell into a particular category—such as information relating to defence—or was held by specific agencies—such as those in the Australian Intelligence Community (AIC)—was not sufficient to justify the protection of the criminal law if disclosure would not, and could not reasonably be expected to, harm specific public interests:

In PIAC’s view, the principles developed under the equitable duty of confidence should be regarded as the touchstone for principled protection of government information. An approach based on the equitable duty of confidence requires a focus on the material in question and the nature of any detriment caused by its release, and

---

<sup>35</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

<sup>36</sup> Ibid.

<sup>37</sup> Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

<sup>38</sup> Australian Federal Police, *Submission SR 33*, 3 March 2009.

has the decided advantage of leaving open an exception where disclosure would expose serious wrongdoing or iniquity.<sup>39</sup>

7.45 PIAC noted the tension between very broad secrecy provisions—such as s 70 of the *Crimes Act*—and the access regime established by the *Freedom of Information Act 1982* (Cth) (the FOI Act), which is limited only by those exceptions and exemptions necessary for the protection of essential public interests and private and business affairs.<sup>40</sup>

7.46 The Department of Human Services (DHS) agreed that the question of harm to the public interest should be considered in light of the Australian Government's approach to freedom of information, but noted that simply stating 'harm to the public interest' in secrecy provisions would not provide sufficient clarity and certainty.<sup>41</sup>

7.47 The Law Council of Australia also noted the tension between criminal secrecy provisions and the FOI Act, stating that it is anomalous that criminal sanctions may be imposed against a public servant who releases Commonwealth information, which a member of the public could successfully request under the FOI Act. The Law Council expressed support for including a harm requirement in secrecy provisions and commented in relation to *R v Kessing*:<sup>42</sup>

It seems reasonably clear that the information contained in the leaked material, whilst confidential and potentially embarrassing to the Sydney Airport Corporation, was not of its nature to be regarded as inherently 'secret', and its release did not cause any obvious harm to the interests of the Commonwealth or to human health or safety. The public debate which followed the charge and conviction of Allan Kessing centred on the public interest in knowing about the standard of security controls at Sydney Airport.<sup>43</sup>

7.48 The Law Council also submitted that:

Whilst it is important that governments are able to maintain secrecy over information that affects national security or national interests (which, properly characterised, tips the balance in favour of collective, rather than individual, rights), the Law Council contends that, in many areas of Executive power, the case for secrecy is far less obvious. Information should only be characterised as 'secret' if its release could reasonably be expected to damage the national interest, where that damage is not outweighed by the public interest in release of the information or ensuring individual rights are not infringed.<sup>44</sup>

39 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009. This view was also expressed by Australia's Right to Know coalition: Australia's Right to Know, *Submission SR 35*, 6 March 2009. The tension between secrecy and FOI is considered in Ch 4.

40 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

41 Department of Human Services, *Submission SR 26*, 20 February 2009.

42 *R v Kessing* [2007] NSWDC 138; *Kessing v The Queen* [2008] NSWCCA 310. This case is discussed in Ch 5.

43 Law Council of Australia, *Submission SR 30*, 27 February 2009.

44 Ibid.

7.49 The Law Council expressed the view that disclosure of information that is merely embarrassing, confidential or sensitive—but does not affect national security, defence, foreign relations or human health or safety—should lead to administrative rather than criminal sanctions.<sup>45</sup>

7.50 The Australian Press Council acknowledged that certain information held by governments needed to be kept confidential, but expressed the view that government information should be available to the public, unless it was foreseeable that disclosure was likely to result in harm to the public interest:

The Council recognises that it may be impractical to abolish all laws restricting access to government information. What the Council seeks is a thorough overhaul of existing legislation to minimise its potential to restrict accountability of government action and to remove, to the greatest extent possible, the legislation's vulnerability to be exploited by governments and officers seeking to evade public scrutiny.<sup>46</sup>

7.51 Whistleblowers Australia agreed, stating that:

In our system of representative government it is essential that the functions and activities of the public sector are as transparent as possible. It is a right of Australian citizens to be as informed as they wish about matters of public administration.<sup>47</sup>

7.52 Australia's Right to Know (ARTK) coalition emphasised the importance of recognising the value of openness, accountability and public ownership of government information, and urged the repeal of s 70 of the *Crimes Act*. The ARTK coalition considered that a principal object of secrecy legislation should be to provide a right of access to information held by government, and that criminal sanctions should only apply to unauthorised disclosures of information where there is an ‘overwhelming public interest in preventing disclosure, and the consequences of disclosure affect national security or public safety’. The ARTK coalition stated that:

In terms of developing the scope of such an exemption, ARTK advocates avoiding, as far as possible, the tendency to rely on the general, preferring an approach whereby specific categories of the public interest are identified and set out in the legislation. Exemptions that are framed in terms of disclosures causing prejudice to the ‘effective workings of government’ or ‘the ordinary course of government’ are too broad, too subjective and risk being construed so widely as to encompass almost any administrative or governmental activity depending on the circumstances.<sup>48</sup>

7.53 A number of stakeholders indicated the areas and information ‘likely to attract an overwhelming public interest against general public disclosure’. For example, the ARTK coalition suggested that it was likely to include information:

---

45 Ibid.

46 Australian Press Council, *Submission SR 16*, 18 February 2009.

47 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

48 Australia's Right to Know, *Submission SR 35*, 6 March 2009.

- relating to intelligence and security operations, terrorism, defence and foreign relations;
- obtained in confidence from, or entrusted in confidence to, other governments or international organisations relating to intelligence and security operations, terrorism, defence and foreign relations;
- relating to operational military matters and national security issues;
- prejudicial to law enforcement, the investigation and prevention of criminal activity or the administration of justice; and
- which could cause harm to any person or prejudice public safety.<sup>49</sup>

7.54 The AGD also identified the types of information that may require protection in the general secrecy offence, including:

- information that could prejudice Australia's national security, defence or international relations;
- information that could endanger life;
- information that could prejudice law enforcement operations and the effective working of law enforcement agencies;
- information provided to the government in confidence by foreign government agencies;
- Cabinet documents; and
- other information that could prejudice the effective working of Government.<sup>50</sup>

7.55 The Australian Securities and Investments Commission (ASIC) submitted that liability should be limited to unauthorised disclosures of information that genuinely requires protection and that is likely to harm the public interest or a private interest:

If an element of injury to public interest was introduced, ASIC agrees that, in the interests of clarity and certainty, the secrecy provisions should be explicit about the public interests they are intended to protect.

---

49 Ibid.

50 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

Finally, if injury to public interest is included as an element, that element should be subject to strict liability. It would be very difficult to prove that a person intended or knew that, their disclosure was likely to harm a specified public interest. The onus should be on that person to prove that he/she neither knew, nor could have been reasonably expected to know, the likely effect of the disclosure.<sup>51</sup>

7.56 In ASIC's view, secrecy provisions and FOI legislation should be complementary. There should be no inherent tension for Commonwealth officers subject to both regimes. In ASIC's experience, it was possible to balance the need to protect certain information under the ASIC secrecy provisions with the need to release information into the public domain under the FOI Act.<sup>52</sup>

### **ALRC's views**

7.57 In the ALRC's view, criminal secrecy provisions should only impose liability on Commonwealth officers for disclosure of Commonwealth information where the disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm. This approach balances the need to protect certain Commonwealth information with the public interest in an open and accountable system of government.

7.58 The ALRC acknowledges that, in some circumstances, the way in which specific secrecy offences are framed, and the context in which they may operate, provide a sufficient likelihood that harm will be caused by an unauthorised disclosure and that an express requirement is unnecessary. This issue is discussed in relation to specific secrecy offences in Chapter 10.

7.59 The proposed new general secrecy offence should, however, expressly include a requirement that the disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm. The proposed general offence applies broadly to all Commonwealth officers and all Commonwealth information. In these circumstances, the harm to the public interest is not implicit and must be made explicit. As discussed in detail in Chapter 13, reg 2.1 of the *Public Service Regulations* takes this approach, regulating disclosure 'if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government'. While this formulation may be appropriate in relation to imposing administrative penalties in the employment context, it is too broad to provide the basis for criminal sanctions.

7.60 In trying to formulate a provision that targets more specific public interests, the ALRC was drawn to the idea that any general secrecy provision should complement the FOI Act. In this regard it is worthwhile noting that the Australian Public Service Commissioner indicates in the *APS Values and Code of Conduct in Practice* that the exemptions in the FOI Act are a useful starting point in determining which categories of information fall within the scope of reg 2.1, in that disclosure has the potential to be

---

51 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

52 Ibid.

prejudicial to the effective working of government.<sup>53</sup> As noted in Chapter 4, the objects clause of the FOI Act states that the Act is intended to extend ‘as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth’:

limited only by exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by departments and public authorities.<sup>54</sup>

7.61 The ALRC has adopted the approach that a subset of the public interests identified in the FOI Act exemptions could inform the development of the public interests to be protected by the proposed general secrecy offence. This would have the additional benefit that FOI guidelines and jurisprudence in relation to the meaning and scope of the various FOI exemptions may assist Commonwealth officers to better understand their obligations under the proposed general secrecy offence.

7.62 In the following section, the ALRC considers which of the FOI exemptions should be reflected in the general secrecy offence. The ALRC notes that, while the FOI Exposure Draft Bill proposes a number of changes to various exemption provisions in the FOI Act—for example, by reformulating the various public interest tests in the existing provisions to a single test that ‘access to the document at the time would, on balance, be contrary to the public interest’—it leaves in place the substance of the exemptions the ALRC has identified for inclusion in the general secrecy offence.<sup>55</sup>

#### **National security, defence and international relations**

7.63 Section 33(1)(a) of the FOI Act provides that a document is exempt if disclosure would, or could reasonably be expected to, cause damage to: the security of the Commonwealth; the defence of the Commonwealth; or the international relations of the Commonwealth.<sup>56</sup> There was general support in submissions, discussed above, for these public interests to be protected by secrecy offences. The ALRC proposes, therefore, that it be an offence under the general secrecy offence to disclose information that causes, is reasonably likely to cause, or is intended to cause harm to the national security, defence or international relations of the Commonwealth.

7.64 The ALRC has some concerns that imposing criminal liability on Commonwealth officers for disclosing information that harms, is reasonably likely to

53 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <[www.apsc.gov.au](http://www.apsc.gov.au)> at 23 September 2008.

54 *Freedom of Information Act 1982* (Cth) s 3(1)(b). The FOI Exposure Draft Bill proposes a revised objects clause—set out in Ch 2—re-emphasising the importance of the right of access.

55 Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 12 (proposed s 11A(5)).

56 Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth) sch 1, cl 5 proposes to repeal the provisions of the FOI Act that permit a minister or delegate to issue a conclusive certificate in relation to documents exempt under s 33(1) of the FOI Act.

harm, or intended to harm Australia's international relations may be too broad. The ALRC notes that some such disclosures may cause embarrassment rather than any significant harm. The FOI Exposure Draft Bill expressly provides that the fact that access to a document could result in embarrassment to the Commonwealth Government, or cause a loss of confidence in the Government, must not be taken into account in deciding whether access to a document would, on balance, be contrary to the public interest.<sup>57</sup> It may be that 'harm to the international relations of the Commonwealth' requires further qualification in the context of the proposed general secrecy offence by providing, for example, that the disclosure had a substantial adverse effect, was reasonably likely to have a substantial adverse effect, or was intended to have a substantial adverse effect on international relations. The ALRC would welcome stakeholder views on this matter.

#### ***Information communicated in confidence by a foreign government***

7.65 Section 33(1)(b) of the FOI Act provides that a document is exempt if disclosure would divulge any information or matter communicated in confidence by or on behalf of a foreign government, an authority of a foreign government or an international organisation, to the Government of the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth or of an authority of the Commonwealth.<sup>58</sup>

7.66 In the ALRC's view, for the purposes of the general secrecy offence, it is not appropriate to protect categories of information. As noted by stakeholders, not every piece of information in any particular category should attract the protection of the criminal law. For this reason, the ALRC has not included this category of information in the proposed general secrecy offence.

7.67 The ALRC recognises, however, that there is an important public interest in protecting the flow of information, and in particular, confidential information, from foreign governments and international organisations. The flow of information between governments and international organisations is an essential element of international relations. In the ALRC's view, if Commonwealth information was disclosed in circumstances that had the potential to, or did in fact, damage the flow of information from foreign governments or international organisations, it would be possible to argue that the disclosure caused, or was reasonably likely to cause, harm to the international relations of the Commonwealth. In this way, the disclosure would be caught by the proposed general secrecy offence.

<sup>57</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 s 11B(4)(a).

<sup>58</sup> Ibid, sch 3 pt 2 cl 11 proposes to insert a new s 4(10) into the FOI Act to clarify that information or communication 'pursuant to any treaty or formal instrument on the reciprocal protection of classified information' is covered by s 33(1)(b) of the FOI Act.

***Relations between the Commonwealth and a state or territory and information communicated in confidence by a state or territory***

7.68 Section 33A of the FOI Act provides that a document is an exempt document if disclosure:

- would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a state; or
- would divulge information or matter communicated in confidence by or on behalf of the Government of a State or an authority of a State, to the Government of the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth or of an authority of the Commonwealth.<sup>59</sup>

7.69 In relation to information that would harm relations between the Commonwealth and the states and territories, the ALRC has formed the view that this public interest is not of the same order as national security, defence and international relations and could be adequately protected by administrative provisions, intergovernmental arrangements and the general law. Section 33A(5) expressly acknowledges that there will be situations in which disclosure of information protected by this exemption will be in the public interest.

7.70 The ALRC has not included ‘harm to relations between the Commonwealth and the states and territories’ in the proposed general secrecy offence, but would be interested in stakeholder views on the issue. In addition, and for the reasons discussed above, the ALRC’s view is that the proposed general secrecy offence should not include protected categories of information. Thus, the offence does not include information communicated in confidence, as described in the second dot point, above.

***Cabinet documents***

7.71 Section 34 of the FOI Act provides that a document is an exempt document if it has been, or will be, submitted to Cabinet for consideration and was brought into existence for the purpose of submission to Cabinet. Other exempt documents in this section include the official records of Cabinet and documents that would involve the disclosure of the deliberations or decisions of Cabinet, other than documents by which

---

<sup>59</sup> Ibid, sch 3 pt 2 cll 23 and 28 propose to repeal s 33A of the FOI Act and enact a new s 47B which would cover the same kind of documents as s 33A(1). However, as ‘conditionally exempt’ documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest. Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth) sch 1 cll 6–7 propose to repeal the provisions of the FOI Act that permit a minister or delegate to issue a conclusive certificate in relation to documents exempt under s 33A(1).

a decision of the Cabinet has been officially published.<sup>60</sup> The ALRC notes the AGD's submission that specific types of information, by their very nature, should be protected and that:

the disclosure of Cabinet documents, regardless of the information contained in them, has the potential to prejudice the effective working of government by diminishing the government's faith that the Cabinet process provides a forum for free and frank debate and consideration of issues.<sup>61</sup>

7.72 As noted above, the ALRC's view is that, in the context of the general secrecy offence, categories of information, as such, should not be protected. In addition, the ALRC's view is that the internal processes of government, including the Cabinet process, are more appropriately protected by administrative processes—such as classification and information-handling guidelines—and the imposition of administrative penalties. The ALRC has not, therefore, included Cabinet documents or the Cabinet process in the proposed new general secrecy offence. If disclosure of a Cabinet document caused, was likely to cause, or was intended to cause harm to one of the specified public interests listed in the general offence, however, this conduct would be caught.

7.73 For the same reasons, the ALRC has not included Executive Council documents,<sup>62</sup> or internal working documents,<sup>63</sup> in the proposed general secrecy offence.

#### ***Enforcement of the criminal law***

7.74 Section 37(1)(a) of the FOI Act provides that a document is an exempt document if disclosure would, or could reasonably be expected to, prejudice the conduct of an investigation of a breach, or possible breach, of the law, or a failure, or possible failure, to comply with a law relating to taxation, or prejudice the enforcement or proper administration of the law in a particular instance. Section 37(1)(b) provides that a document is an exempt document if disclosure would, or could reasonably be

---

60 The Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 23 proposes to repeal and replace s 34 of the FOI Act. The new provision would clarify that the Cabinet exemption is limited to documents prepared for the dominant purpose of submission for the consideration of Cabinet. The Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth) sch 1 cl 8 proposes to repeal the provisions of the FOI Act that permit the Secretary of the Department of the Prime Minister and Cabinet to issue a conclusive certificate in relation to documents exempt under s 34.

61 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

62 *Freedom of Information Act 1982* (Cth) s 35. The Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 23 proposes to repeal s 35.

63 *Freedom of Information Act 1982* (Cth) s 36. Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 23, 28 propose to repeal s 36 of the FOI Act and enact a new s 47C in its place. Proposed s 47C would cover the same kind of documents as s 36(1). However, as 'conditionally exempt' documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest. Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008 (Cth) sch 1 cl 10 proposes to repeal the provisions of the FOI Act that permit a minister or delegate to issue a conclusive certificate in relation to documents exempt under s 36(1).

expected to disclose, or enable a person to ascertain, the existence or identity of a confidential source of information, or the non-existence of a confidential source of information, in relation to the enforcement or administration of the law.

7.75 In its submission to this Inquiry, the Australian Commission for Law Enforcement Integrity (ACLEI) emphasised the sensitive nature of some of the information it receives:

Those who would give information in secret to law enforcement agencies are commonly concerned for their own safety, particularly against reprisals from those whose interests could be adversely affected by the information they provide.

These people seek assurance that their information will not be disclosed, whether through inadvertence or corruption. While the details of the measures law enforcement agencies take to keep information confidential are of little interest to these people, what matters is the reputation of an agency for being able to keep secrets.<sup>64</sup>

7.76 ACLEI noted that it was essential to protect the flow of information to the agency, ‘whether it comes from other government agencies, from business, from informers, from covert surveillance activities, or from ordinary members of the public’. ACLEI noted the well-established link between the unauthorised disclosure of information and police corruption, such as the disclosure of information alerting suspects to police raids; disclosing the presence or identity of police informers; and disclosing the use or methods of surveillance or other techniques used to investigate criminal activity.

Anti-corruption agencies, such as ACLEI, take a central role in government’s investment in ensuring that particularly sensitive law enforcement information is not compromised by unauthorised disclosure by individuals as a consequence of their corrupt conduct.<sup>65</sup>

7.77 The ALRC’s view is that the disclosure of information that causes, is likely to cause, or intended to cause harm to ongoing criminal investigations—including disclosing the identity of confidential sources of information—should be covered by the proposed general secrecy offence. The formulation in s 37 appears, however, to be too wide for this purpose in that it extends to ‘the proper administration of the law in a particular instance’.

7.78 Information Privacy Principle (IPP) 11 in the *Privacy Act 1988* (Cth) provides an exemption for disclosures of personal information that are reasonably necessary for the enforcement of the criminal law, or of a law imposing a pecuniary penalty, or for

---

<sup>64</sup> Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

<sup>65</sup> Ibid.

the protection of the public revenue.<sup>66</sup> National Privacy Principle (NPP) 2 provides an exemption for disclosures that organisations believe are reasonably necessary for one or more of the following by or on behalf of an ‘enforcement body’:<sup>67</sup>

- the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;
- the enforcement of laws relating to the confiscation of the 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 implementation of the orders of a court or tribunal.<sup>68</sup>

7.79 The ALRC has adopted the formulation set out in part in NPP 2 to describe the law enforcement public interest to be protected by the general secrecy offence. The proposal below focuses on the first three categories listed in NPP 2: the enforcement of the criminal law and laws relating to the confiscation of the proceeds of crime, and protection of the public revenue. The ALRC would be interested in feedback from stakeholders on this issue.

7.80 The ALRC has not included a public interest based on the exemption set out in s 37(2)(a) of the FOI Act—that is, where disclosure would, or could reasonably be expected to prejudice the fair trial of a person or the impartial adjudication of a particular case. This is because the courts have their own procedures for protecting their processes and may impose their own penalties for such conduct.

#### ***Endangering the life or physical safety of any person***

7.81 Section 37(1)(c) of the FOI Act provides that a document is an exempt document if disclosure would, or could reasonably be expected to endanger the life or physical safety of any person. The ALRC agrees with stakeholders that a disclosure of Commonwealth information that endangered, was reasonably likely to endanger, or intended to endanger the life or physical safety of any person should be covered by the proposed general secrecy offence.

---

66 Privacy Act 1988 (Cth) s 14. Broadly speaking, the IPPs regulate the conduct of public sector agencies. The NPPs regulate the conduct of private sector organisations.

67 Ibid s 6 sets out a definition of ‘enforcement body’, which includes the AFP, the ACC, APRA, and ASIC.

68 Ibid sch 3.

7.82 A somewhat broader approach might be based on the language used in NPP 2: ‘a serious threat to an individual’s life, health or safety’. The ALRC would be interested in stakeholder views on how best to formulate this harm for the purposes of the proposed new general secrecy offence, and whether the offence should cover disclosures that ‘pose a serious threat to an individual’s life, health or safety’.

#### ***Prejudice the protection of public safety***

7.83 Section 37(2)(c) of the FOI Act provides that a document is an exempt document if disclosure would, or could reasonably be expected to, prejudice the maintenance or enforcement of lawful methods for the protection of public safety. In the ALRC’s view, while disclosures that cause, are reasonably likely to cause, or intended to cause harm to public safety should be covered by the proposed general secrecy offence, the formulation in s 37(2)(c) may be too narrow. Again, a somewhat broader description of the relevant public interest can be found in NPP 2 and the ALRC has adopted this model: ‘a serious threat to public health or public safety’.

#### ***Documents to which secrecy provisions apply***

7.84 Section 38 of the FOI Act provides that a document is an exempt document if disclosure of the document, or information contained in the document, is prohibited under a provision of an enactment; and the provision is specified in sch 3 of the FOI Act; or s 38 is expressly applied to the document, or information, by the provision, or by another provision of that or any other enactment. The relationship between s 38 and secrecy provisions is discussed in detail in Chapter 4.

#### ***Documents concerning certain operations of agencies***

7.85 Section 40 of the FOI Act provides that a document is exempt if its disclosure would, or could reasonably be expected to impact adversely on the conduct of agency operations. Examples of such adverse impact include:

- prejudice to the effectiveness of procedures or methods for the conduct of tests, examinations or audits by an agency;
- a substantial adverse effect on the management or assessment of personnel by the Commonwealth or by an agency;
- a substantial adverse effect on the proper and efficient conduct of the operations of an agency; or

- a substantial adverse effect on the conduct by or on behalf of the Commonwealth or an agency of industrial relations.<sup>69</sup>

7.86 These are matters relating to the internal management and operations of agencies, and should be addressed through administrative procedures and, where necessary, the imposition of administrative penalties. This is also the ALRC's view in relation to the exemption set out in s 43A of the FOI Act relating to research undertaken by officers of agencies.<sup>70</sup>

### ***Personal privacy***

7.87 Section 41 of the FOI Act provides that a document is exempt if its disclosure would involve 'the unreasonable disclosure of personal information about any person (including a deceased person)'.<sup>71</sup> It is possible to argue that harm to personal privacy should not be included in the general secrecy offence. The *Privacy Act* provides individuals with an avenue to pursue government agencies and others where personal information is disclosed in breach of the IPPs or NPPs, and administrative, contractual and general law obligations may also apply. The disclosure of personal information does not, generally, attract criminal sanctions outside the public sector.

7.88 A number of stakeholders expressed strong views in relation to this issue. For example, the AGD submitted that:

There is a legitimate expectation that personal information provided by the public to government agencies will be kept confidential. While the harm in disclosing such personal information may be minimal in an individual case, the negative impact it has on the confidence of the public to provide this information is significant. Criminal sanctions provide an important deterrent and send a strong message that the unauthorised use or disclosure of personal information is unacceptable.<sup>72</sup>

7.89 As discussed in Chapter 4, the AGD noted that privacy and secrecy, while related, are distinct areas of the law. Privacy law regulates the behaviour of agencies and organisations, while secrecy laws are intended to prevent unauthorised disclosure of sensitive, government-held information, and are intended to regulate the behaviour

---

69 Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cll 24, 28 propose to repeal s 40 of the FOI Act and enact a new s 47E in its place. Proposed s 47E would cover the same kind of documents as s 40 with the exception of documents currently covered by s 40(e) regarding an adverse effect on the conduct by or on behalf of the Commonwealth or an agency of industrial relations. As 'conditionally exempt' documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest.

70 Ibid, sch 3 pt 2 cll 24, 28 propose to repeal s 43A of the FOI Act and enact a new s 47H in its place. Proposed s 47H would cover the same kind of documents as s 43A. However, as 'conditionally exempt' documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest.

71 Ibid, sch 3 pt 2 cll 24, 28 proposes to repeal s 41 of the FOI Act and enact a new s 47F in its place. Proposed s 47F would cover similar kinds of documents as s 41. However, as 'conditionally exempt' documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest.

72 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

of individuals. The AGD noted that some overlap existed, but that the processes and remedies available under the *Privacy Act*, which are aimed at agencies and organisations, do not have the same deterrent effect for individual Commonwealth officers.<sup>73</sup>

7.90 A number of agencies that handle large amounts of personal information, including the DHS and the Department of Education, Employment and Workplace Relations (DEEWR), also emphasised the potential damage to individuals and the Commonwealth where personal information is disclosed, as well as the value of the deterrent effect of criminal penalties.<sup>74</sup>

7.91 The Treasury expressed the view that:

The taxation law imposes criminal sanctions for the unauthorised disclosure of taxpayer information. Treasury considers that this is appropriate given the purpose that the secrecy provisions have in deterring their breach, as well as providing taxpayers with the confidence that their information is subject to a high level of protection.<sup>75</sup>

7.92 The ARTK coalition stated that:

it does not seem incompatible for civil and administrative remedies to apply along with concurrent criminal penalties applicable under separate legislation, such as the *Crimes Act 1914*, in circumstances where the unauthorised use or disclosure of personal information may also constitute a serious breach of secrecy laws. This circumstance would be analogous to a person's concurrent civil and criminal liability for assault, trespass or damage to property.<sup>76</sup>

7.93 The ALRC's view is that unauthorised disclosure of personal information generally should not attract criminal penalties. There is a range of other remedies available—including individual complaints to the Privacy Commissioner under the *Privacy Act* and administrative, contractual and general law remedies—that are a more appropriate response to such disclosure.

7.94 The ALRC has, however, considered the concern expressed by agencies about the ability of the Australian Government to collect personal information from the Australian community. Agencies have suggested that the potential to impose criminal penalties for unauthorised disclosure of personal information supports community confidence in the ability of the Government to protect the information. The ALRC proposes, therefore, to include personal privacy as one of the public interests to be protected by the general secrecy offence in certain circumstances. In order to attract

---

73 Ibid.

74 Department of Human Services, *Submission SR 26*, 20 February 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

75 The Treasury, *Submission SR 22*, 19 February 2009.

76 Australia's Right to Know, *Submission SR 35*, 6 March 2009.

criminal penalties, however, the ALRC proposes that the harm that is caused, reasonably likely to be caused, or intended to be caused by a disclosure of information that impacts on personal privacy should be of a relatively high order, that is, the disclosure would have to have a substantial adverse effect on personal privacy.

### ***Trade secrets and business, commercial, financial affairs of persons and organisations***

7.95 Section 43 of the FOI Act provides that a document is an exempt document if its disclosure would disclose a trade secret or any other information having a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were disclosed; or other information concerning a person in respect of his or her business or professional affairs or concerning the business, commercial or financial affairs of an organisation or undertaking, being information the disclosure of which:

- would, or could reasonably be expected to, unreasonably affect that person adversely in respect of his or her lawful business or professional affairs or that organisation or undertaking in respect of its lawful business, commercial or financial affairs; or
- could reasonably be expected to prejudice the future supply of information to the Commonwealth or an agency for the purpose of the administration of a law of the Commonwealth or of a Territory or the administration of matters administered by an agency.<sup>77</sup>

7.96 Generally, the ALRC's view is that harm to business, commercial or financial affairs should not attract criminal penalties where the disclosure does not involve fraud.<sup>78</sup> There is a range of other remedies available to address unauthorised disclosure of this kind of information including administrative, contractual and general law remedies. The ALRC agrees with the ARTK coalition that:

Currently a large number of secrecy provisions, if breached, are punishable by imprisonment, notwithstanding the relative triviality of the offence and in many cases they merely seek to protect what can be described as information that is no more than commercial in confidence. Criminal sentences are not appropriate in such circumstances. . . .

In a commercial context, the disclosure of confidential information does not attract such a severe regime and the civil remedies (such as damages or dismissal) are

<sup>77</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 24 and 28 propose to repeal s 43 of the FOI Act and enact a new s 47G in its place. Proposed s 47G would cover similar kinds of documents as s 43. However, as 'conditionally exempt' documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest.

<sup>78</sup> Section 142.2 of the *Criminal Code* includes an offence for the use of Commonwealth information with the intention of dishonestly obtaining a benefit or dishonestly causing a detriment to another person.

adequate to deter a breach of the duty of confidence. The same should apply in the public sector.<sup>79</sup>

7.97 A number of stakeholders expressed the view that damage to these interests should be covered, however, on the basis that disclosure of such information had the potential to prejudice the future supply of information to the Commonwealth. The Department of Climate Change, for example, submitted that:

Commonwealth secrecy provisions should aim to protect information which could have a negative commercial impact on commercial entities (such as providing an unfair advantage to a competitor) or other persons if inappropriately disclosed.<sup>80</sup>

7.98 APRA noted that information collected from regulated entities is often ‘commercially sensitive’ and, therefore:

from the perspective of a strong and robust prudential supervision regime it is important that APRA’s extensive information-gathering powers ... be accompanied by a robust secrecy provision.<sup>81</sup>

7.99 Similarly, the Australian Competition and Consumer Commission (ACCC) stated that, in contrast to many Commonwealth departments and agencies, the ACCC is mainly concerned with ‘commercially sensitive’ information, the disclosure of which ‘may have a substantial adverse effect on the information provider’.<sup>82</sup>

7.100 The ALRC proposes, therefore, to include the protection of business, commercial or financial affairs of individuals and organisations as one of the public interests to be protected by the general secrecy offence, in certain circumstances. In order to attract criminal penalties, however, the ALRC proposes that the harm caused, reasonably likely to be caused, or intended to be caused should be of a relatively high order, that is, the disclosure would have to have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.

#### ***Financial or property interests of the Commonwealth***

7.101 Section 39 of the FOI Act provides that a document is exempt if its disclosure would have a substantial adverse effect on the financial or property interests of the Commonwealth or of an agency.<sup>83</sup> As noted above, the ALRCs view is that, generally,

79 Australia’s Right to Know, *Submission SR 35*, 6 March 2009.

80 Department of Climate Change, *Submission SR 27*, 23 February 2009.

81 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

82 Australian Competition & Consumer Commission, *Submission SR 11*, 12 February 2009.

83 Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 24 and 28 propose to repeal s 39 of the FOI Act and enact a new s 47D in its place. Proposed s 47D would cover the same kinds of documents as s 39. However, as ‘conditionally exempt’ documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest.

disclosure of this kind of Commonwealth information should not attract criminal sanctions where it would not attract such sanctions outside the public sector. The ALRC has not included this public interest in the general secrecy offence on the basis that, unlike disclosure of personal and commercial information affecting the interests of members of the Australian community, disclosure of such information would not have an adverse impact on the ability of the Commonwealth to collect information.

#### ***Adverse effect on managing the economy***

7.102 Section 44 of the FOI Act provides that a document is exempt if its disclosure would, or could reasonably be expected to:

- have a substantial adverse effect on the ability of the Government of the Commonwealth to manage the economy of Australia; or
- result in an undue disturbance of the ordinary course of business in the community, or an undue benefit or detriment to any person or class of persons, by reason of giving premature knowledge of or concerning proposed or possible action or inaction of the Government or Parliament of the Commonwealth.<sup>84</sup>

7.103 The Australian Government Solicitor's *Freedom of Information Guidelines* note in relation to s 44 that:

It is the consequences of disclosure that are significant when determining whether a document is exempt under s 44, not the nature of the document or the information contained in the document (although they are likely to be relevant considerations). The expected effect of disclosure must be on the government's ability to manage the economy. These words seem to suggest that the effect must be on the process of decision making in relation to the economy, rather than on the economy itself.<sup>85</sup>

7.104 The ALRC has not included these public interests in the proposed general secrecy provision on the basis that damage to the decision-making processes of government should generally be dealt with on an administrative basis. In addition, the *Criminal Code* already includes criminal offences for the use of Commonwealth information with the intention of dishonestly obtaining a benefit or dishonestly causing a detriment to another person.<sup>86</sup> The ALRC would, however, be interested in stakeholder views in relation to this issue.

84 Ibid, sch 3 pt 2 cll 24 and 28 propose to repeal s 44 of the FOI Act and enact a new s 47J in its place. The proposed s 47J differs from s 44 and would exempt documents that would, or could reasonably be expected to, have a substantial adverse effect on Australia's economy by influencing a decision or action of a person or entity, or by giving a business an undue benefit or detriment by providing premature knowledge of proposed or possible action or inaction by a person or entity. As 'conditionally exempt' documents, under the proposed amendments an agency or minister must give a person access to these documents unless it would be contrary to the public interest.

85 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2007) <[www.dpmc.gov.au](http://www.dpmc.gov.au)> at 14 October 2008, [16.1.3].

86 *Criminal Code* (Cth) s 142.2.

***Material obtained in confidence***

7.105 Section 45 of the FOI Act provides that a document is exempt if its disclosure would found an action for breach of confidence. In the ALRC's view, disclosure of information that would found such an action should be dealt with under the general law dealing with breach of confidence, or under administrative provisions. This section describes a category of information, rather than a public interest, and should not be included in the general criminal offence.

***Sections 42, 46, 47 and 47A***

7.106 Sections 42, 46, 47 and 47A of the FOI Act deal with the disclosure of documents: which would be privileged from production in legal proceedings on the ground of legal professional privilege; which would amount to a contempt of court, or would infringe the privileges of parliament; arising out of certain elements of the companies and securities legislation;<sup>87</sup> and the electoral roll and related documents, respectively. In the ALRC's view, these should not be included in the general secrecy offence. The courts and the Australian Parliament have procedures in place to deal with unauthorised disclosure of documents, including the imposition of penalties.

7.107 In relation to the documents protected by ss 47 and 47A, in the ALRC's view, the documents relating to the Ministerial Council for Companies and Securities and the National Companies and Securities Commission should be protected by administrative arrangements between the Commonwealth and the states and territories. The electoral roll and related documents are regulated by specific secrecy provisions. The circumstances in which specific secrecy provisions may be justified are discussed in Chapters 10 to 12.

**Proposal 7–1** The proposed general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:

- (a) harm the national security, defence or international relations of the Commonwealth;
- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;

<sup>87</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 3 pt 2 cl 27 proposes to repeal s 47 of the FOI Act relating to the disclosure of information arising out of certain companies and securities legislation.

- (c) endanger the life or physical safety of any person;
- (d) pose a serious threat to public health or public safety;
- (e) have a substantial adverse effect on personal privacy; or
- (f) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.

### **Fault element attaching to harm**

7.108 The *Criminal Code* provides that fault elements may include intention, knowledge, recklessness or negligence, but that particular offences may specify other fault elements.<sup>88</sup> As noted in Chapter 5, under the *Code*, if the legislation creating an offence does not specify a fault element for a physical element consisting of conduct, the fault element is intention.<sup>89</sup> Where an offence provision does not specify a fault element for a physical element consisting of a circumstance or a result, the fault element is recklessness.<sup>90</sup>

7.109 In Chapter 8, the ALRC proposes that the fault element attaching to the physical element of disclosure of Commonwealth information should be intention. It is also necessary to consider what fault element should attach to the physical element of harm to the specified public interests in the context of the general secrecy offence.

7.110 For the purposes of the *Criminal Code*, harm to specified public interests can be characterised as a ‘result’. Thus, if no fault element is specified, the *Criminal Code* will impose recklessness as the fault element.

<b>Physical element</b>	<b>Fault element</b>
Conduct = disclosure of Commonwealth information	Intention
Result = the disclosure caused, or was reasonably likely to cause harm to a specified public interest	Recklessness

<sup>88</sup> *Criminal Code* (Cth) s 5.1. For example, the *Criminal Code* itself stipulates an additional fault element of ‘dishonesty’ in relation to offences in Ch 7—*The Proper Administration of Government*. Dishonesty is defined as ‘dishonest according to the standards of ordinary people’ and ‘known by the defendant to be dishonest according to the standards of ordinary people’: s 130.3.

<sup>89</sup> *Ibid* s 5.6(1).

<sup>90</sup> *Ibid* s 5.6(2).

7.111 Section 5.4 of the *Criminal Code* provides in part that:

- (2) A person is reckless with respect to a result if:
  - (a) he or she is aware of a substantial risk that the result will occur; and
  - (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
- (3) The question whether taking a risk is unjustifiable is one of fact.
- (4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

7.112 In these circumstances, the proposed general secrecy offence would consist of an intentional disclosure of Commonwealth information, by a Commonwealth officer who was reckless as to whether or not the identified harms would result from the disclosure. Under s 5.4(4) the offence would also address situations in which the officer knew the harm would result or intended that the harm would result.

#### ***Strict liability and absolute liability***

7.113 Strict liability and absolute liability offences do not require any fault elements to be proved. The difference between them is that the defence of an honest and reasonable mistake of fact is available in relation to strict liability offences, but not available in relation to absolute liability offences.<sup>91</sup> Courts are unlikely to impose strict or absolute liability unless there is a clear and express indication in the legislation.<sup>92</sup>

7.114 The *Guide to Framing Commonwealth Offences* notes that the default position under the *Criminal Code* reflects the common law premise that:

it is generally neither fair, nor useful, to subject people to criminal punishment for unintended actions or unforeseen consequences unless those resulted from an unjustifiable risk (ie recklessness).<sup>93</sup>

7.115 The *Guide* goes on to indicate, however, that the application of strict or absolute liability to a particular physical element may be appropriate where there is evidence that a requirement of proving fault in relation to that physical element could undermine the deterrent effect of the offence.<sup>94</sup>

7.116 The Senate Standing Committee for the Scrutiny of Bills has also noted that the requirement for a fault element is one of the most fundamental protections of the criminal law, and that strict liability offences should only be introduced after careful

---

<sup>91</sup> Ibid ss 6.1, 6.2. See also *Proudman v Dayman* (1941) 67 CLR 536.

<sup>92</sup> *He Kaw Teh v R* (1985) 157 CLR 523.

<sup>93</sup> Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 24.

<sup>94</sup> Ibid, 25.

consideration and on a case by case basis.<sup>95</sup> The Standing Committee concluded that strict liability may be appropriate where it has proved difficult to prosecute fault provisions, particularly those involving intent. The Committee noted that strict liability had been applied in a range of circumstances, including where it is difficult for the prosecution to prove a fault element because a matter was peculiarly within the knowledge of the defendant.<sup>96</sup>

7.117 The Senate Standing Committee also concluded that:

two-tier or parallel offences are acceptable only where the strict liability limb is subject to a lower penalty than the fault limb, and to other appropriate safeguards; in addition, it should be clearly evident that the fault limb alone would not be sufficient to effect the purpose of the provision.<sup>97</sup>

7.118 An example of an offence provision that attaches strict liability to one element of the offence is s 58 of the *Defence Force Discipline Act*. The provision provides that strict liability applies to the requirement that the disclosure is likely to be prejudicial to the security or defence of Australia. The application of strict liability avoids the evidential difficulties for the prosecution in proving beyond reasonable doubt that the accused was reckless as to whether, or knew, or intended that, the disclosure was likely to be prejudicial to the security or defence of Australia. The provision also provides a defence where the accused can prove that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to be prejudicial to the security or defence of Australia.

### ***Submissions and consultations***

7.119 In IP 34, the ALRC asked in what circumstances it would be appropriate to have fault elements other than intent and recklessness in secrecy provisions.<sup>98</sup> The AGD noted that difficulty in proving an offence usually arises in relation to fault elements applicable to circumstances or results and submitted that:

Strict liability may be appropriate where it is necessary to ensure the integrity of a regulatory regime such as those relating to public health and safety, the environment, or financial or corporate regulation. An example of this is regulation 132(3) of the *Civil Aviation Regulations 1988* (Cth), which prevents unauthorised disclosure of information relating to air traffic reports received by the Civil Aviation Safety Authority. Absolute liability offences are rare and should be limited to jurisdictional or similar elements of offences that are not relevant to the person's culpability.

Application of strict or absolute liability to a particular physical element of an offence has generally only been considered appropriate where one of the following considerations is applicable:

---

95 Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002), 283.

96 Australian Parliament—Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002), 259.

97 Ibid, 285.

98 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–6.

- there is demonstrated evidence that the requirement to prove fault of that particular element is undermining or will undermine the deterrent effect of the offence, and there are legitimate grounds for penalising persons lacking ‘fault’ in respect of that element, or
- in the case of absolute liability, there should also be legitimate grounds for penalising a person who made an honest and reasonable mistake of fact in respect of that element.<sup>99</sup>

7.120 The AGD suggested that an objective test, such as that used in reg 2.1 of the *Public Service Regulations*, would be the preferred approach in relation to the requirement to prove harm.<sup>100</sup>

7.121 On the other hand, the Australian Press Council stated that secrecy offences should never be strict liability or absolute liability offences. Rather:

In all instances the minimum requirement for a conviction should be that the offender knew that the information was confidential, knew that he or she had a duty not to disclose the information, a reasonable expectation that the disclosure would be likely to cause damage to the public interest and that such damage would be more than merely trivial or an embarrassment to the government or to a public official. Before a criminal conviction should be imposed there should be a finding, either that there was an intention to cause harm to a specified public interest, or recklessness as to the probability of such harm occurring.<sup>101</sup>

7.122 Liberty Victoria expressed the view that criminal liability should only attach to behaviour that is reckless or intentional, and that in other circumstances—such as unintentional mishandling of official information—only administrative penalties should apply.<sup>102</sup>

7.123 The Treasury noted that some taxation secrecy offences do contain strict liability elements. However, in considering the consolidation of tax secrecy provisions, Treasury did not consider that there was any reason to depart from the default elements outlined in the *Criminal Code*.<sup>103</sup>

7.124 PIAC suggested that:

a defence should be available where, at the time of the alleged offence, a person did not know, and would not reasonably have believed, that the information, document or article in question contained protected subject matter, disclosure of which would cause significant damage or prejudice to the public interest.<sup>104</sup>

---

99 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

100 Ibid.

101 Australian Press Council, *Submission SR 16*, 18 February 2009.

102 Liberty Victoria, *Submission SR 19*, 18 February 2009.

103 The Treasury, *Submission SR 22*, 19 February 2009.

104 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

7.125 Whistleblowers Australia made a similar point, stating that:

If the disclosure was inadvertent or unintentional and not reckless, then serious consideration must be given to those facts and any penalties reduced or removed accordingly.

However, if a person deliberately discloses information with the foreknowledge that such a disclosure will cause or will be likely to cause actual or real harm to the public interest or a specific public interest, then an appropriate penalty should be imposed.<sup>105</sup>

#### *ALRC's views*

7.126 In Chapter 8, the ALRC proposes that the conduct covered by the general secrecy offence should be disclosure of Commonwealth information, and that the fault element attaching to that physical element of the offence should be intention. In this chapter the ALRC proposes that there be three tiers to the general secrecy offence as follows:

#### *First Tier*

<b>Physical element</b>	<b>Fault element</b>
Conduct = disclosure of Commonwealth information	Intention
Result = the disclosure caused, or was reasonably likely to cause, harm to one or more of the specified public interests	Strict Liability

#### *Second Tier*

<b>Physical element</b>	<b>Fault element</b>
Conduct = disclosure of Commonwealth information	Intention
Result = the disclosure did, was reasonably likely to, or intended to: <ul style="list-style-type: none"> <li>• have a substantial adverse effect on personal privacy; or</li> <li>• have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.</li> </ul>	Recklessness, knowledge, or intention

---

105 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

*Third Tier*

<b>Physical element</b>	<b>Fault element</b>
Conduct = disclosure of Commonwealth information	Intention
<p>Result = the disclosure did, or was reasonably likely to, or intended to:</p> <ul style="list-style-type: none"> <li>• harm the national security, defence or international relations of the Commonwealth;</li> <li>• prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;</li> <li>• endanger the life or physical safety of any person; or</li> <li>• pose a serious threat to public health or public safety.</li> </ul>	Recklessness, knowledge or intention

7.127 The ALRC notes that there will often be evidential difficulties—in relation to the second and third tier offences set out above—in establishing that a Commonwealth officer was reckless as to whether—or knew or intended that—the unauthorised disclosure would cause harm to one of the specified public interests. For this reason, the ALRC proposes that there be a first tier offence that attaches strict liability to the harm requirement. In this case, the offence will be committed where a Commonwealth officer intentionally discloses information, and the disclosure actually harms, or is reasonably likely to harm, one or more of the specified public interests. It will not be necessary to prove any fault in relation to this result, only that it was reasonably likely to occur.

7.128 This is consistent with the ALRC’s previous recommendation in *Keeping Secrets*, that secrecy provisions should apply only to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.<sup>106</sup> This approach also recognises that Commonwealth officers have access to Commonwealth information because they hold positions of trust in the community.

---

106 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

Such positions involve a level of responsibility to take care that information that harms, or could potentially harm, the public interest, is not disclosed.

7.129 Under s 6.1 of the *Criminal Code*, the defence of mistake of fact will be available in relation to the first tier offence. ‘Mistake of fact’ means that, at or before the time of the offence, the person considered whether or not facts existed, and acted under a mistaken but reasonable belief about those facts.<sup>107</sup> The ALRC also proposes that there be a defence to this offence provision, modelled on s 58 of the *Defence Force Discipline Act*, in circumstances where the person can prove that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to harm any of the specified public interests. The defendant will bear the legal burden in relation to this defence.

7.130 In addition, the ALRC proposes that there be two upper tiers with recklessness, knowledge or intention attaching to the harm element. In relation to these two tiers, an offence will be committed where a Commonwealth officer intentionally discloses information, and is reckless as to whether, or knows or intends that, the disclosure will result in harm to one or more of the specified public interests. These tiers will attract higher penalties than the first tier strict liability offence. The third tier offence will attract higher penalties than the second tier offence on the basis of the type of public interests protected by the third tier offence. Essentially, the third tier offence involves harm to the Australian community or to an individual’s life or safety, while the second tier offence involves harm to individual privacy or commercial interests. These issues and the proposed penalties for all three tiers of the offence are discussed in Chapter 9.

**Proposal 7–2** The proposed general secrecy offence should consist of three tiers, as follows:

- (a) **First tier:** the unauthorised disclosure caused, or was reasonably likely to cause, harm to one or more of the specified public interests. Strict liability attaches to this result.
- (b) **Second tier:** the Commonwealth officer was reckless as to whether, or knew or intended that, the disclosure would:
  - (i) have a substantial adverse effect on personal privacy; or
  - (ii) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.

107 *Criminal Code* (Cth) s 9.2.

- (c) **Third tier:** the Commonwealth officer was reckless as to whether, or knew or intended that, the disclosure would:
- (i) harm the national security, defence or international relations of the Commonwealth;
  - (ii) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
  - (iii) endanger the life or physical safety of any person; or
  - (iv) pose a serious threat to public health or public safety.

**Proposal 7–3** The first tier offence should include a defence in circumstances where the Commonwealth officer can prove that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to harm any of the specified public interests.



## 8. General Secrecy Offence: Elements

---

### Contents

Introduction	259
Whose conduct should be regulated?	260
‘Commonwealth officers’ and others	261
‘Commonwealth public officials’	262
Australian Public Service employees and others	263
Contracted service providers	265
The Governor-General	267
Ministers and parliamentary secretaries	268
Members of the Houses of Parliament	269
Commonwealth judicial officers	270
Former Commonwealth officers	272
ALRC’s views	274
Initial and subsequent disclosures	276
Submissions and consultations	278
ALRC’s views	280
What conduct should be regulated?	282
Receiving information	283
Copying, recording and using information	284
Disclosing, divulging, communicating	286
ALRC’s views	287
Fault element attaching to disclosure	288
What information should be protected?	290
ALRC’s views	291

### Introduction

8.1 As discussed in Chapter 6, the ALRC is proposing that ss 70 and 79(3) of the *Crimes Act 1914* (Cth) be repealed and that a new general secrecy offence should be enacted in the *Criminal Code* (Cth).<sup>1</sup> In the Issues Paper, *Review of Secrecy Laws* (IP 34),<sup>2</sup> the ALRC sought stakeholder views on how such an offence should be framed.<sup>3</sup> This chapter considers some of the essential elements of the proposed new

---

<sup>1</sup> Sections 70 and 79(3) are described in detail in Chs 5 and 6, and set out in full in Appendix 5.

<sup>2</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

<sup>3</sup> Ibid, Question 2–2.

offence—including whose conduct, and what kind of conduct, should be regulated. Chapter 9 goes on to consider what exceptions and defences should be available under the proposed general secrecy offence, and what penalties should apply for breach.

## **Whose conduct should be regulated?**

8.2 Chapter 5 provides an overview of the parties regulated by federal secrecy provisions. As noted in that chapter, secrecy provisions can apply to:

- Commonwealth officers;
- specific Commonwealth agencies;
- organisations or individuals providing services for or on behalf of the Commonwealth;
- other specific categories of organisations or individuals; or
- ‘any person’.

8.3 Section 70 of the *Crimes Act* applies to ‘Commonwealth officers’, as defined in s 3 of that Act. Section 79(3) of the *Crimes Act* regulates the conduct of ‘any person’. The *Criminal Code* includes a number of offences concerning the conduct of Commonwealth public officials.<sup>4</sup> The term ‘Commonwealth public official’ is defined in the *Criminal Code*, and includes elements from all three arms of government—the legislature, the executive and the judiciary. In this chapter, the ALRC considers whether the proposed general secrecy offence, to be included in the *Criminal Code*, should regulate the behaviour of ‘Commonwealth public officials’ as defined in the *Code*, or a smaller group of ‘Commonwealth officers’ defined separately for the purposes of the proposed new offence.

8.4 The answer will depend on whether the offence is intended essentially to regulate the activity of the executive branch of the Australian Government, or whether it is intended to operate more broadly. In Chapter 2, the ALRC considers the structures established by the *Australian Constitution* and the doctrine of the separation of powers. The ALRC’s proposed approach in relation to the new general secrecy offence is to focus on disclosure of Commonwealth information by members of the executive branch of government.

---

<sup>4</sup> These include the offence of ‘Abuse of Public Office’ that, in part, prohibits public officials from using any information that the official has obtained in the official’s capacity as a public official with the intention of dishonestly obtaining a benefit for himself or herself or for another person; or dishonestly causing a detriment to another person: *Criminal Code* (Cth) s 142.2.

8.5 The following section examines each of the elements in the definitions of ‘Commonwealth officer’ in the *Crimes Act* and ‘Commonwealth public official’ in the *Criminal Code* and the extent to which these overlap. The ALRC then considers which elements should be covered by the proposed new general secrecy offence.

### ‘Commonwealth officers’ and others

8.6 The term ‘Commonwealth officer’ is defined in the *Crimes Act* to mean:

- a person holding office under, or employed by, the Commonwealth, and includes:
- (a) a person appointed or engaged under the *Public Service Act 1999*;
  - (aa) a person permanently or temporarily employed in the Public Service of a Territory or in, or in connection with, the Defence Force, or in the Service of a public authority under the Commonwealth;
  - (b) the Commissioner of the Australian Federal Police, a Deputy Commissioner of the Australian Federal Police, an [Australian Federal Police] employee or a special member of the Australian Federal Police (all within the meaning of the *Australian Federal Police Act 1979*); and
  - (c) for the purposes of section 70, a person who, although not holding office under, or employed by, the Commonwealth, a Territory or a public authority under the Commonwealth, performs services for or on behalf of the Commonwealth, a Territory or a public authority under the Commonwealth; and
  - (d) for the purposes of section 70:
    - (i) a person who is an employee of the Australian Postal Corporation;
    - (ii) a person who performs services for or on behalf of the Australian Postal Corporation; and
    - (iii) an employee of a person who performs services for or on behalf of the Australian Postal Corporation.<sup>5</sup>

8.7 The definition is fairly broad and although there is some uncertainty at the outer limits, as discussed below, it clearly covers: Australian Public Service (APS) employees; others employed by or holding office under the Commonwealth; those who perform services for or on behalf of the Commonwealth; and those employed by ‘public authorities’, defined as ‘any authority or body constituted by or under a law of the Commonwealth or of a Territory’. The definition also specifically covers the Australian Federal Police (AFP), the Australian Defence Forces (ADF) and the Australian Postal Corporation.

8.8 In order for s 70 of the *Crimes Act* to apply, it is necessary for a person to fall within the definition of ‘Commonwealth officer’ in s 3 and, in addition, to be subject to a duty of non-disclosure as discussed in detail in Chapter 7.

---

<sup>5</sup> *Crimes Act 1914* (Cth) s 3.

8.9 Section 79(3) of the *Crimes Act* applies to any person who discloses prescribed information where the information has come to them in certain circumstances. These circumstances are set out in 79(1), and include where information:

has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he or she has made or obtained it owing to his or her position as a person:

- (i) who is or has been a Commonwealth officer;
- (ii) who holds or has held office under the Queen;
- (iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth;
- (iv) who is or has been employed by or under a person to whom a preceding subparagraph applies; or
- (v) acting with the permission of a Minister;

and, by reason of its nature or the circumstances under which it was entrusted to him or her or it was made or obtained by him or her or for any other reason, it is his or her duty to treat it as secret ...

8.10 This provision extends liability for disclosure of Commonwealth information beyond Commonwealth officers, office holders and contractors to include any person—including, potentially, a journalist—who acquires such information in circumstances which give rise to a duty to treat the information as secret. As discussed in detail, below, the ALRC proposes that, in some circumstances, the subsequent disclosure of Commonwealth information by any person who receives the information knowing, or having reasonable grounds to believe, that the information has been disclosed in breach of the general secrecy offence should also be an offence.<sup>6</sup>

### **‘Commonwealth public officials’**

8.11 The term ‘Commonwealth public official’ is defined comprehensively in the Dictionary to the *Criminal Code* and includes paragraphs (a) to (t).<sup>7</sup> The Revised Explanatory Memorandum for the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth) states, in relation to this definition, that:

‘Commonwealth public official’ includes a broad group of people including Commonwealth employees and officers, Members of Parliament, judges, police, contractors, military personnel and those employed by Commonwealth authorities.<sup>8</sup>

8.12 The definition ‘sets the scope of the protection of the theft, fraud, bribery and related offences which are to assist with the proper administration of government’.<sup>9</sup> The definition includes bodies established ‘by or under a law of the Commonwealth’

---

<sup>6</sup> See Proposal 8–3.

<sup>7</sup> The definition is set out in full in Appendix 5.

<sup>8</sup> Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [367].

<sup>9</sup> Ibid, [367].

created to perform government functions. These are captured by the term ‘Commonwealth authority’, which is defined separately. The Explanatory Memorandum notes that the current definition of ‘public authority under the Commonwealth’ in s 3 of the *Crimes Act*, which includes any authority or body constituted by or under a law of the Commonwealth or of a Territory, ‘lacks sufficient discrimination’.<sup>10</sup>

8.13 A number of bodies and organisations are expressly excluded because they are separate from the Commonwealth government. These include Aboriginal councils and associations; the ACT, Northern Territory and Norfolk Island Governments; corporations and bodies such as registered unions and employer associations.<sup>11</sup>

### Australian Public Service employees and others

8.14 The following elements are taken from the definition of ‘Commonwealth public official’. They cover APS employees and other public sector employees and there is a significant degree of overlap with the definition of ‘Commonwealth officer’ in the *Crimes Act*:

- APS employees;
- other individuals employed by the Commonwealth otherwise than under the *Public Service Act*;
- members of the ADF;
- members or special members of the AFP;
- individuals who hold or perform the duties of an office established by or under a law of the Commonwealth;
- officers and employees of Commonwealth authorities, as defined in the *Criminal Code*; and
- individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth.

8.15 These elements represent the key working units of the executive branch of government that is responsible for collecting, generating and controlling the flow of Commonwealth information. The extent to which these elements cover judicial officers is discussed further below.

---

10 Ibid, [367].

11 See eg *Criminal Code* (Cth) Dictionary definition of ‘Commonwealth public official’ paras n and r.

### ***Submissions and consultations***

8.16 In IP 34, the ALRC asked when secrecy provisions should regulate the behaviour of persons other than Commonwealth officers.<sup>12</sup> A number of stakeholders raised the possibility that the proposed general secrecy offence should regulate the activity of any person who comes into possession of Commonwealth information in certain circumstances. The Australian Government Attorney-General's Department (AGD) submitted that:

it may be appropriate for secrecy laws to apply to anyone who comes into possession of the relevant information where the potential damage of unauthorised disclosure would be particularly grave. It may be in the public interest for secrecy provisions to regulate the behaviour of 'any person' for information that could prejudice national security, defence, international relations, or put individuals at risk of harm.<sup>13</sup>

8.17 The Australian Intelligence Community (AIC) was also of this view, stating that:

The AIC considers there may be merit in extending the offence in section 70 of the *Crimes Act* to all persons. AIC agencies note that the damage to national security (whether danger to life and liberty of staff members and agents; or other critical information disclosure) can be severely affected if disseminated by the media or in other public fora.<sup>14</sup>

8.18 On the other hand, the Australian Taxation Office (ATO) submitted that the taxation secrecy provisions should regulate only those within government agencies, or those performing services for such an agency, except where information has been disclosed to, or obtained by, a person in breach of a taxation law.<sup>15</sup>

### ***ALRC's views***

8.19 In the ALRC's view, the primary focus of the proposed general secrecy offence should be the protection of Commonwealth information collected or generated by the executive branch of government. The executive collects and generates vast amounts of information from and about individuals and organisations on both a compulsory and voluntary basis and it is this sector that is the main focus of s 70 of the *Crimes Act*. The ALRC proposes that 'Commonwealth officer' be defined for the purposes of the new general secrecy offence, and that the definition should include APS employees and other public sector employees by reference to those elements of the definition of 'Commonwealth public official' set out above.

8.20 In addition, however, the ALRC proposes a new offence for subsequent disclosure of Commonwealth information where a person knows, or has reasonable grounds to believe, that the information has been disclosed by a Commonwealth officer

---

12 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–1.

13 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

14 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

15 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

in breach of the general secrecy offence. The proposed new subsequent disclosure offence is discussed in detail below, and will include an additional requirement that the person knew, was reckless as to whether, or intended, that the disclosure would harm one of the public interests listed in the general secrecy offence.

8.21 It is possible to distinguish between the offences set out in the *Criminal Code*, such as bribery and abuse of public office—that apply to ‘Commonwealth public officials’—and the proposed general secrecy offence that is intended to protect information collected and generated by the executive. The existing *Criminal Code* offences are directed at corruption in public office, while the proposed general secrecy offence is directed at protecting information collected and generated by government. For this reason, the ALRC is of the view that it is not appropriate to rely on the definition of ‘Commonwealth public official’ in the *Criminal Code* to define those who are subject to the proposed general secrecy offence. Instead, ‘Commonwealth officer’ should be defined separately for the purposes of the proposed new offence.

### Contracted service providers

8.22 Currently, the definition of ‘Commonwealth officer’ in s 3 of the *Crimes Act* includes ‘a person who … performs services for or on behalf of the Commonwealth, a Territory or a public authority under the Commonwealth’. This paragraph was added to the definition in 1987, in order to reflect the changing and increasingly dispersed nature of government and government service provision.<sup>16</sup> It recognises that Commonwealth information is often handled by those contracted to provide goods and services to or on behalf of the Commonwealth.

8.23 The Revised Explanatory Memorandum for the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill notes that the definition of ‘Commonwealth public official’ in the *Criminal Code* also extends to Commonwealth contracted service providers, that is:

those who provide services by contract rather than as an office holder or employee ... Often these people have responsibilities that are indistinguishable from departmental officers. While they are covered by the *Crimes Act 1914* definition of ‘Commonwealth officer’ for some offences (non-disclosure, theft, falsification or records, corruption, impersonation and obstruction—sections 75 to 76), there is no reason why they should not be subject to the full range of Chapter 7 offences (including the fraud related offences).

The definition of ‘contracted service provider’ covers parties to a contract with a ‘Commonwealth entity’ but also subcontractors. Often it is the subcontractors who provide the services.<sup>17</sup>

---

<sup>16</sup> *Statute Law (Miscellaneous Provisions) Act 1987* (Cth) sch 1. This issue is discussed further in Ch 3.

<sup>17</sup> Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [371]–[372].

8.24 The definition of ‘Commonwealth public official’ in the *Criminal Code* Dictionary includes:

- individuals who are contracted service providers for a Commonwealth contract; and
- individuals who are officers or employees of a contracted service provider for a Commonwealth contract and who provide services for the purposes (whether direct or indirect) of the Commonwealth contract.

8.25 The term ‘contracted service provider for a Commonwealth contract’ is also defined in the *Criminal Code* to mean a person who is a party to the Commonwealth contract and who is responsible for the provision of services to a Commonwealth entity under the Commonwealth contract; or a subcontractor for the Commonwealth contract.

8.26 These provisions are specifically directed to individuals, rather than entities. There is an argument, in the context of the proposed general secrecy offence, that entities which are contracted service providers should also be subject to the general criminal offence. The Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) (the Tax Laws Exposure Draft Bill) includes, as part of the proposed definition of a ‘taxation officer’, ‘an entity engaged to provide services relating to the ATO (such as cleaning firms or IT contractors) and any individual employed or subcontracted by such an entity’.<sup>18</sup>

### ***Submissions and consultations***

8.27 There was considerable support in submissions for ensuring that the proposed general secrecy offence continued to cover Commonwealth contracted service providers.<sup>19</sup> The Department of Human Services (DHS), for example, stated that:

The extent of outsourcing and potential partnerships with non-Commonwealth entities makes it necessary that secrecy laws bind [contracted service providers] and partners as if they were Commonwealth employees. The Department notes that, in respect of personal information, this is consistent with s 95B and IPP 4 of the Privacy Act, which require that contracted service providers are held to the same privacy standards that would have applied if the service or function they are performing for or on behalf of an agency had been performed by the agency itself.<sup>20</sup>

---

<sup>18</sup> Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 355-25. The contractual relationship between the Australian Government and contracted service provider entities and individuals is discussed in detail in Ch 14.

<sup>19</sup> Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; Australian Federal Police, *Submission SR 33*, 3 March 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

<sup>20</sup> Department of Human Services, *Submission SR 26*, 20 February 2009.

8.28 The Treasury provided the following example:

Treasury considers that it is appropriate that secrecy obligations have a wide application to reflect the reality that private individuals and entities are increasingly being used to assist in the provision of government services. In the taxation context, a clear example is the use of debt collection agencies to assist with the collection of outstanding taxation debt. Although disclosed outside of a Commonwealth Government agency, the sensitivity of the information is not diminished, nor is the policy justification for ensuring a high level of protection of that information.<sup>21</sup>

#### ***ALRC's views***

8.29 The ALRC agrees that Commonwealth contracted service providers should be covered by the proposed new general secrecy offence. This reflects the reality that contracted services providers are increasingly involved in the business of government, including the provision of government services. They collect and generate large amounts of information, which would clearly be Commonwealth information if it was collected or generated by an Australian Government agency, and this information should be protected in the same way by the criminal law whether it happens to be held by the public or private sector.

8.30 Consequently, the ALRC proposes that the definition of ‘Commonwealth officer’ for the purposes of the general secrecy offence should include individuals and entities who are contracted service providers under a Commonwealth contract. The ALRC is of the view that contracted entities should also be subject to the deterrent value of the criminal law. This will encourage such entities to ensure that appropriate measures are put in place to protect Commonwealth information. The general secrecy offence should extend to officers and employees of contracted service providers and to sub-contractors.

#### **The Governor-General**

8.31 The Revised Explanatory Memorandum for the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill states that:

The definition of ‘Commonwealth officer’ in subsection 3(1) of the *Crimes Act 1914* is very unsatisfactory. This is because there have even been doubts expressed in the past that it covers Ministers and it does not even cover the Governor-General. It is critical that all people who perform duties and functions for the Commonwealth are covered. This is not only relevant to corruption offences, but the whole range of Chapter 7 offences.<sup>22</sup>

---

21 The Treasury, *Submission SR 22*, 19 February 2009.

22 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [371].

8.32 It appears that the Governor-General does not fall within the definition of ‘Commonwealth officer’ in the *Crimes Act*, and so would not be liable to prosecution under s 70. The Governor-General would, however, be liable to prosecution under s 79(3) of the *Crimes Act*, in appropriate circumstances, as the provision applies to any person. The Governor-General belongs to the executive branch of government and has access to Commonwealth information at the highest level. Although the Governor-General is not currently subject to s 70 of the *Crimes Act*, it is arguable that the activity of the Governor-General should be regulated by the proposed general secrecy offence.

8.33 The Governor-General’s staff are appointed or employed under the *Governor-General Act 1974* (Cth) and will, therefore, be covered by other elements of the definition of ‘Commonwealth public official’. The Governor-General’s Official Secretary, for example, is ‘an individual who holds or performs the duties of an office established by or under a law of the Commonwealth’ and other staff will be individuals ‘employed by the Commonwealth otherwise than under the *Public Service Act*’. As discussed above, it is the ALRC’s view that these elements should be included in the definition of ‘Commonwealth officer’ for the purposes of the general secrecy offence.

### **Ministers and parliamentary secretaries**

8.34 As noted in the Revised Explanatory Memorandum for the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill there is some doubt whether the definition of ‘Commonwealth officer’ in the *Crimes Act* extends to cover ministers. By way of contrast, however, Lindgren J in *Wong v Minister for Immigration and Multicultural and Indigenous Affairs* reasoned that they should be covered:

The expression ‘Commonwealth officer’ is defined in s 3 of the *Crimes Act 1914* to mean ‘a person holding office under, or employed by, the Commonwealth’, and to include particular office-holders listed in the definition. Section 64 of the *Constitution* empowers the Governor-General to appoint ‘officers’ to administer departments of State of the Commonwealth, and provides that ‘[s]uch officers shall hold office during the pleasure of the Governor-General’.<sup>23</sup>

8.35 Ministers and parliamentary secretaries belong to the executive branch of government and have access to Commonwealth information at the highest level. Although there is some uncertainty, ministers may be subject to prosecution under s 70 where they are subject to a duty of non-disclosure, as well as more specific secrecy offence provisions, such as s 150 of the *Child Support (Assessment) Act 1989* (Cth), which expressly applies to the Minister. Both ministers and parliamentary secretaries are also potentially subject to prosecution under s 79(3) of the *Crimes Act*. It is certainly arguable, therefore, that the activity of ministers and parliamentary secretaries should be regulated by the new general secrecy offence.

---

23       *Wong v Minister for Immigration and Multicultural and Indigenous Affairs* (2004) 204 ALR 722, 744.

8.36 On the other hand, where ministers are not expressly prohibited from disclosing information, they may be required to decide whether certain Commonwealth information should be disclosed or not. Information may be disclosed on the basis of a decision by the minister that disclosure is generally in the public interest, even though the disclosure may cause harm to a particular public interest—for example, Australia's relationship with another country. John McGinness noted that:

Sections 70 and 79(3) do not specify who may authorise the disclosure of information. A committee which reviewed equivalent provisions in the United Kingdom suggested that in practice authorisation for this purpose is implied, flowing from the nature of public servants' duties. It accepted that Ministers and 'senior' civil servants are self-authorising.<sup>24</sup>

8.37 The ALRC proposes that, for the purposes of the proposed general secrecy offence, the definition of 'Commonwealth officer' should include ministers and parliamentary secretaries. In order to address the issue of disclosures authorised by the minister, the ALRC proposes in Chapter 9 that one of the exceptions to the new general secrecy offence should be disclosure with the approval of an agency head or the responsible minister, who would have to certify that disclosure is in the public interest in any particular case.<sup>25</sup>

8.38 In his submission, James Renwick suggested that:

although public servants are often blamed for the leaking of information, it is widely suspected that most leaks of information come from the offices of ministers, usually from their staff (who, these days, are rarely public servants). Any criminal or civil law sanctions imposed to prevent leaking by public servants ought equally apply to ministerial staffers.<sup>26</sup>

8.39 Ministerial staff are generally employed under the *Members of Parliament (Staff) Act 1984* (Cth) and will, therefore, be individuals 'employed by the Commonwealth otherwise than under the *Public Service Act*'. The ALRC proposes to include such individuals in the definition of 'Commonwealth officer' for the purposes of the new general secrecy offence. Although the proposed exception for approval by the minister will allow information to be disclosed by ministerial staff, this will not protect ministers' staff from prosecution for unauthorised 'leaks' where information is disclosed that harms, is reasonably likely to harm, or is intended to harm, the public interests discussed in Chapter 7.

## Members of the Houses of Parliament

8.40 Members of the Australian Parliament, both Senators and Members of the House of Representatives, who are not ministers or parliamentary secretaries, do not form part of the executive branch of government, but are part of the legislative branch.

---

<sup>24</sup> J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 62.

<sup>25</sup> Proposal 9–1(b).

<sup>26</sup> J Renwick, *Submission SR 02*, 11 December 2008.

While Members of Parliament do not fall within the definition of ‘Commonwealth officer’ in s 3 of the *Crimes Act*, they are expressly included in the definition of ‘Commonwealth public official’ in the *Criminal Code*. On occasion they do have access to Commonwealth information that is not in the public domain, for example, when they are approached by whistleblowers or briefed on government proposals. Members of Parliament would be liable to prosecution for unauthorised disclosure of such information under s 79(3) of the *Crimes Act*, in appropriate circumstances.

8.41 The proposed general secrecy offence targets Commonwealth information held by Commonwealth officers. The ALRC does not propose to extend the definition of Commonwealth officer beyond the executive branch to include Members of Parliament who are not ministers or parliamentary secretaries, although the ALRC would be interested in feedback from stakeholders on this issue. Members of Parliament may be liable to criminal penalties if in breach of the ALRC’s proposed subsequent disclosure provision.<sup>27</sup>

8.42 In addition, Members of Parliament are liable to criminal penalties for breach of existing provisions of the *Criminal Code*. These include provisions that prohibit a Commonwealth public official from using any information that he or she has obtained in the official’s capacity as an official with the intention of dishonestly obtaining a benefit for himself or herself or for another person, or dishonestly causing a detriment to another person.<sup>28</sup>

### **Commonwealth judicial officers**

8.43 The Revised Explanatory Memorandum for the Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill states that:

Certain judicial officers are covered by the *Crimes Act 1914* definition of ‘Commonwealth officer’ (subsection 3(1)) which covers any person holding office under the Commonwealth. This would include judges of federal courts but there is less certainty about the status of judicial registrars, and State and Territory judges and officials performing judicial functions.<sup>29</sup>

8.44 Judicial officers, when acting judicially, do not form part of the executive branch of government, but comprise the judicial branch. As discussed in Chapter 2, the *Australian Constitution* establishes the principle of the separation of powers, meaning that the three functions of government—the power to make laws, administer laws and decide disputes—are conferred on three different bodies: the legislative, executive and the judiciary. The independence of the judicial branch and the strict separation of judicial power, established under Chapter III of the *Australian Constitution*, is fundamental to Australia’s system of representative democracy. General secrecy

---

27 Proposal 8–3.

28 *Criminal Code* (Cth) s 142.2.

29 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [370].

provisions must not, therefore, interfere with, or limit, the exercise of federal judicial power by a federal court.

8.45 It is possible to confer executive functions on judicial officers—acting as designated persons rather than in their judicial capacity—for example, the power to issue warrants under the *Telecommunications (Interception and Access) Act 1979* (Cth). As noted in Chapter 2, in *Grollo v Palmer*, Gummow J expressly considered this situation and the fact that judicial officers might be subject to prosecution under s 70 for breach of a duty of non-disclosure arising under the *Telecommunications (Interception and Access) Act* or, possibly, under s 79 of the *Crimes Act*. Although in this case, Gummow J expressed the view that the ambit of the duty imposed by these provisions ‘stops short of impeding discharge of the higher duty flowing from Chapter III of the Constitution’, he noted that:

But for this construction which, in my view, should be placed upon the Act and upon ss 70 and 79 of the *Crimes Act*, I would have accepted the submission by the applicant that the impugned provision of the Act and these sections of the *Crimes Act*, in their operation upon information and documents acquired by ‘eligible Judges’ pursuant to the Act, did amount to an impermissible undermining of the *Boilermakers* doctrine.<sup>30</sup>

8.46 In addition, judicial officers are liable to criminal penalties for breach of existing provisions of the *Criminal Code*, including s 142.2 on misuse of official information by Commonwealth public officials, discussed above.<sup>31</sup>

#### *ALRC’s views*

8.47 Although both the legislative and judicial branches collect information from individuals and organisations on both a voluntary and compulsory basis, the context in which this information is collected and used is quite different from the executive branch. Much of the information is collected in the context of public processes, such as court hearings and parliamentary committee inquiries. These processes raise different issues in relation to disclosure of information, and have their own rules and procedures for providing protection for information in appropriate circumstances. It is also possible to make specific provision in legislation regarding disclosure of certain executive branch information to the judicial and legislative branches of government and this has been done in a number of existing secrecy provisions.<sup>32</sup>

8.48 The proposed general secrecy offence targets Commonwealth information held by Commonwealth officers in the executive branch of government. The ALRC is not proposing that the definition of Commonwealth officer for the purposes of the proposed offence be extended beyond the executive branch to include judicial officers acting in their judicial capacity. However, judicial officers may be liable under the

---

30 *Grollo v Palmer* (1995) 184 CLR 348, 398.

31 *Criminal Code* (Cth) s 142.2.

32 See eg *Migration Act 1958* (Cth) s 46A(5) re disclosure to the Australian Parliament; and *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 90(4) re disclosure to the courts.

proposed general secrecy offence when appointed as designated persons to perform executive functions under Commonwealth legislation, the extent that this was consistent with the exercise of federal judicial power as discussed above.<sup>33</sup>

8.49 In addition, the ALRC proposes the enactment of an offence relating to the subsequent disclosure of Commonwealth information by any person, where the person knows, or has reasonable cause to believe, that the information has been disclosed in breach of the general secrecy offence.<sup>34</sup> This proposed offence would apply to any person including, potentially, those working in the judicial and legislative branches of government. The offence would, however, be subject to the operation of the *Australian Constitution*, including the doctrine of the separation of powers and the requirement not to interfere with the exercise of judicial power, and the doctrine of parliamentary privilege.<sup>35</sup>

### **Former Commonwealth officers**

8.50 Chapter 5 considers the extent to which existing secrecy provisions expressly regulate the behaviour of former Commonwealth officers and others who have had access to Commonwealth information in the past, but no longer have access. For example, s 70 of the *Crimes Act* expressly regulates the behaviour of persons who are Commonwealth officers,<sup>36</sup> as well as those who have been Commonwealth officers.<sup>37</sup>

8.51 As noted in Chapter 5, the common law duty of fidelity and loyalty also provides some protection for information acquired during the employment relationship once that relationship ends. Leo Tsaknis noted that the common law duty allows former employees to use the knowledge, skills and experience gained as an employee in order to carry out their profession or trade, while also protecting confidential information where disclosure would have an adverse impact on the employer's business.<sup>38</sup>

8.52 Tsaknis argued, however, that s 70(2) of the *Crimes Act* does not draw a distinction between information that is confidential and information that is not, and expressed the view that this imposes 'a form of servitude that the common law would not countenance'.<sup>39</sup> Paul Finn agreed with this view, stating that this provision is 'objectionably wide in its scope and mysterious in its possible applications'.<sup>40</sup> Finn's view was that third party and commercial information should be protected—while it remains confidential and not in the public domain—but suggested that, in relation to

---

33 Proposal 8–3.

34 Proposal 8–3.

35 See Ch 2.

36 *Crimes Act 1914* (Cth) s 70(1).

37 Ibid s 70(2).

38 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 262.

39 Ibid.

40 P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 259.

other government information, it should only be protected to the extent that disclosure is likely to injure the public interest.<sup>41</sup>

### **Submissions and consultations**

8.53 In IP 34, the ALRC sought stakeholder views on the circumstances in which it is appropriate for secrecy provisions to continue to regulate the behaviour of those who have been Commonwealth officers, or who have held other positions subject to Commonwealth secrecy provisions, but who are no longer in those positions.<sup>42</sup> In response, the AGD submitted that:

If there are strong reasons for protecting information based upon its nature and the harm to the public interest if it is disclosed, it would seem to follow that secrecy laws should extend, in most cases, to individuals who formerly held positions where they were required to keep the relevant information confidential. To exclude such persons from the ambit of secrecy laws would frustrate their purpose, as it would allow a person to avoid any penalty simply by resigning from the relevant office before making an unauthorised disclosure.<sup>43</sup>

8.54 Stakeholders agreed that it would significantly undermine the utility of the provisions if they did not extend to former officers.<sup>44</sup> The Australian Prudential Regulation Authority (APRA), for example, noted that the effectiveness of its secrecy provision would be ‘dramatically curtailed if it did not apply to former officers’.<sup>45</sup>

8.55 The Australian Securities and Investments Commission (ASIC) noted that, if a secrecy provision included a ‘harm to the public interest’ test, this would allow former Commonwealth officers to disclose certain information, for example, where the information had become dated and was no longer relevant to the operations of the agency.<sup>46</sup>

### **ALRC’s views**

8.56 The ALRC’s view is that the proposed general secrecy offence should apply to both current and former Commonwealth officers. The ALRC agrees with stakeholders that it would significantly undermine the utility of the provision if it did not extend to former officers. This problem is especially acute in relation to those who have had access to highly sensitive information in the Australian Intelligence Community or the law enforcement context. The requirement, discussed in Chapter 7, that to attract

---

41 Ibid, 257.

42 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–3.

43 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

44 Australian Intelligence Community, *Submission SR 37*, 6 March 2009; NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

45 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

46 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

criminal liability any disclosure must cause harm, be reasonably likely to cause harm, or be intended to cause harm will limit the liability of former Commonwealth officers, consistent with Finn's analysis, discussed above.

### **ALRC's views**

8.57 The ALRC considers that the following 'Commonwealth officers' should be covered by the proposed new general secrecy offence:

- the Governor-General;
- Ministers and parliamentary secretaries;
- APS employees—that is, individuals appointed or engaged under the *Public Service Act*;
- individuals employed by the Commonwealth otherwise than under the *Public Service Act*;
- members of the ADF;
- members or special members of the AFP;
- individuals who hold or perform the duties of an office established by or under a law of the Commonwealth;
- officers or employees of Commonwealth authorities;
- individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth.
- individuals and entities who are contracted service providers for a Commonwealth contract; and
- individuals who are officers or employees of a contracted service provider for a Commonwealth contract and who provide services for the purposes (whether direct or indirect) of the Commonwealth contract.

8.58 The ALRC's view is that the proposed new offence should not apply to judicial officers acting in their judicial capacity, or to members of parliament who do not form part of the executive. It may be necessary to expressly exclude judicial officers from the definition of 'Commonwealth officer'.

8.59 These elements have been adapted from the definition of 'Commonwealth public official' in the *Criminal Code*. There are a number of express exceptions to

these elements in the *Code* that will also need to be included in the definition of ‘Commonwealth officer’ for the purposes of the general secrecy offence, such as individuals who hold or perform the duties of an office established under, for example, the *Corporations Act 2001* (Cth) or the ACT and Northern Territory self-government Acts.<sup>47</sup>

**Proposal 8–1** The proposed general secrecy offence should regulate the conduct of those who are, or have been, ‘Commonwealth officers’; defined as follows:

- (a) the Governor-General;
- (b) ministers and parliamentary secretaries;
- (c) Australian Public Service employees, that is, individuals appointed or engaged under the *Public Service Act 1999* (Cth);
- (d) individuals employed by the Commonwealth otherwise than under the *Public Service Act*;
- (e) members of the Australian Defence Force;
- (f) members or special members of the Australian Federal Police;
- (g) individuals who hold or perform the duties of an office established by or under a law of the Commonwealth;
- (h) officers or employees of Commonwealth authorities;
- (i) individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth;
- (j) individuals and entities who are contracted service providers for a Commonwealth contract; and
- (k) individuals who are officers or employees of a contracted service provider for a Commonwealth contract and who provide services for the purposes (whether direct or indirect) of the Commonwealth contract.

<sup>47</sup> *Criminal Code* (Cth) Dictionary.

**Proposal 8–2** The proposed general secrecy offence should *not* regulate the conduct of judicial officers exercising the judicial power of the Commonwealth, or Members of the Australian Parliament who are not ministers or parliamentary secretaries.

## Initial and subsequent disclosures

8.60 As noted in Chapter 5, a number of existing secrecy provisions regulate both the initial disclosure, whether authorised or unauthorised, and any subsequent unauthorised disclosure of Commonwealth information. The majority of secrecy offences mapped by the ALRC, however, do not contain a prohibition on subsequent unauthorised disclosure. McGinness notes that:

Where a secrecy provision permits disclosure to other government agencies then, in the absence of a specific provision, the persons receiving the information are not bound by that statute to maintain its confidentiality ... Some secrecy provisions attempt to deal with this by imposing a further prohibition on disclosure by recipients.<sup>48</sup>

8.61 The Tax Laws Exposure Draft Bill has addressed this problem by proposing three separate offences to cover the following possibilities:

- the unauthorised disclosure of taxpayer information by current and former taxation officers;
- the unauthorised disclosure of taxpayer information by individuals who receive the information as a result of a lawful disclosure; and
- the unauthorised disclosure of taxpayer information by individuals who receive the information as a result of an unlawful disclosure.<sup>49</sup>

8.62 The proposed taxation provision provides that an entity does not commit an offence if the information was obtained with authority—that is, under one of the disclosure exceptions—and the information is on-disclosed for, or in connection with, the original purpose of disclosure.<sup>50</sup> However, an offence is committed where information is on-disclosed and the subsequent disclosure does not fall within one of the exceptions to the prohibition on disclosure.<sup>51</sup> The following example is provided in the Explanatory Material:

48 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 64.

49 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.9].

50 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 s 355-175.

51 Ibid sch 1 item 1 s 355-155.

Paul, an employee of the Australian Prudential Regulation Authority, receives taxpayer information from the ATO for the purposes of administering the *Superannuation Industry (Supervision) Act 1993* (SIS Act). Paul discloses the information to a journalist and to another Australian Prudential Regulation Authority employee for a purpose that is unconnected to the administration of the SIS Act. In both cases, the disclosure of the information is an offence.<sup>52</sup>

8.63 When Commonwealth information is disclosed without authority, the action for breach of confidence may provide a remedy. An action can be brought against a third party to whom information has been communicated in breach of a duty of confidence where that third party was aware, or should reasonably have been aware, that the information was confidential.<sup>53</sup>

8.64 In 1995, the House of Representatives Standing Committee report, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (the *In Confidence* report), expressed the view that the general offence provisions should also prohibit unauthorised dealing in confidential third party information at every point in the ‘distribution chain’, where there was the requisite mental element.<sup>54</sup>

8.65 The earlier *Review of the Commonwealth Criminal Law*, developed by a committee chaired by Sir Harry Gibbs (the Gibbs Committee), recommended that Australian legislation should follow the model provided by the *Official Secrets Act 1989* (UK), and include a provision prohibiting subsequent unauthorised disclosures. The Gibbs Committee recommended the following form of words for the offence:

[W]here a person knows, or has reasonable grounds to believe, that information—

- (i) had been disclosed (whether to him or another) by a Commonwealth officer or government contractor without authority or had been unlawfully obtained from either such person; or
- (ii) had been entrusted to him or her in confidence by such officer or contractor on terms requiring it to be held in confidence; or
- (iii) had been disclosed (whether to him or another) without lawful authority by a person to whom it had been entrusted as in (ii);

it would be an offence for the person to disclose the information without authority, knowing or having reasonable cause to believe that the disclosure would be damaging.<sup>55</sup>

---

52 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.32].

53 The equitable action for breach of confidence in relation to Commonwealth information is discussed in Ch 5.

54 Australian Parliament—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), [7.11.7].

55 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 333.

### **Submissions and consultations**

8.66 In IP 34, the ALRC asked whether secrecy provisions should, as a matter of course, include offences dealing with both the initial unauthorised handling of information and any subsequent disclosures.<sup>56</sup> There was significant support in submissions for covering both initial and subsequent unauthorised disclosures, in particular, where the person making the subsequent unauthorised disclosure knew, or was reckless as to whether, the information had been initially disclosed without authority.

8.67 The ATO submitted that the taxation secrecy provisions should apply where information has been disclosed to, or obtained by, a person in breach of a taxation law. This is the position under s 8XB of the *Taxation Administration Act 1953* (Cth):

In the absence of these types of provisions, the ATO would be concerned that protected information could be released in breach of a secrecy provision and that information could subsequently be used (by the media for example) without that subsequent use being subject to any criminal sanction.<sup>57</sup>

8.68 The AGD stated that:

Arguably, if information is sensitive and it is in the public interest for it to be protected from unauthorised disclosure, then it may be appropriate to regulate both initial and subsequent unauthorised disclosure. It would be important to ensure that this did not cover inadvertent or unintentional disclosures by the second person. It may be appropriate for any offence of subsequent unauthorised disclosure to include additional elements requiring proof that the person knew, or was aware of the substantial risk, that the information was provided to them in breach of the law and that they had reason to believe that they should not further disclose the information. Consideration might also be given to cases where a person knows, or is aware of the substantial risk, that disclosure might cause harm, but has not necessarily turned his or her mind to whether the initial disclosure was lawful or not.<sup>58</sup>

8.69 The AFP agreed that secrecy offence provisions should cover subsequent use of information where the subsequent user knew, or should have known, that the information had been disclosed on an unlawful basis or was classified or protected and should not be further used or disclosed.<sup>59</sup>

8.70 The Treasury made clear that it supported regulating both initial and subsequent disclosure and that the same penalties should apply to both. The Treasury stated that ‘maintaining the integrity of the information becomes no less important notwithstanding the information may have been on-disclosed a number of times’.<sup>60</sup>

---

56 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–5.

57 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

58 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

59 Australian Federal Police, *Submission SR 33*, 3 March 2009.

60 The Treasury, *Submission SR 22*, 19 February 2009.

8.71 A range of other stakeholders agreed that secrecy provisions should cover subsequent use or disclosure.<sup>61</sup> ASIC added, however, that secrecy provisions should not extend to the unauthorised, but unsolicited, receipt and possession of Commonwealth information.<sup>62</sup>

8.72 The Public Interest Advocacy Centre (PIAC) also expressed concern about imposing criminal liability for receipt of information:

In PIAC's view, criminal liability should only apply to third parties who knowingly deal with secret material with the intention of damaging the defence or security of Australia. ... PIAC believes that the penalties for subsequent handling should be of a lower order, except where intent to damage Australia's national interest is proven.<sup>63</sup>

8.73 In its submission, the Australian Press Council asserted that in many, if not most instances 'when the media publish information that has been leaked from government, there is some element of public interest involved'. In addition, the Press Council noted that journalists and editors are not subject to the same legislative and administrative duties as Commonwealth officers:

A journalist will have a different set of professional obligations and does not have the same training in information assessment. This raises difficulties, which need to be considered when framing secrecy legislation. Because media professionals are not subject to the disciplinary processes, which are available in relation to public servants, a situation may arise where a minor disclosure that is ostensibly in the public interest is treated as a breach of secrecy warranting criminal conviction. By contrast, a public servant making a disclosure of the same information for the same purpose might instead be disciplined by way of a range of internal mechanisms, even though the duty breached is arguably a higher one than that breached by the journalist.<sup>64</sup>

8.74 The Press Council suggested that specific provision should be made in secrecy provisions in relation to unauthorised disclosures to journalists. The Council noted that the conduct of media organisations 'in the course of journalism' is exempt from the National Privacy Principles in the *Privacy Act* on condition that the organisation is publicly committed to observe published privacy standards. The Press Council suggested that a similar exemption could operate in relation to secrecy provisions where media organisations were committed to a set of standards dealing with the handling of confidential government information:

Such standards would specify that journalists must not publish government information that they know to be confidential unless there is a sincerely held belief

---

61 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

62 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

63 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

64 Australian Press Council, *Submission SR 16*, 18 February 2009.

that publication would be in the public interest. The Press Council would be willing to cooperate with government agencies in the drafting of appropriate standards.<sup>65</sup>

### **ALRC's views**

8.75 Although most existing secrecy provisions do not seek to address subsequent unauthorised disclosures, the ALRC can see merit in the argument that the general secrecy offence should cover subsequent disclosures in certain circumstances. The ALRC agrees that, in the context of the proposed new general secrecy provision, it would not be appropriate to criminalise the mere receipt of Commonwealth information—even where the information has been disclosed in contravention of the provision—if there is no subsequent disclosure. Those who receive such information should have the opportunity to inform the relevant agency and, possibly—as in the Centrelink example provided by the DHS above—to return the information.

8.76 However, where a person receives Commonwealth information knowing, or reckless as to whether, the information has been disclosed in breach of the general secrecy offence and then intentionally on-discloses that information knowing, intending, or reckless as to whether, the disclosure would harm, or was reasonably likely to harm, one of the identified public interests, it appears reasonable to impose criminal sanctions.

8.77 As discussed in Chapter 7, the proposed general secrecy offence is limited to the disclosure of information that will harm, is reasonably likely to harm, or is intended to harm specific and important public interests. In these circumstances, it is the ALRC's view that it would not be appropriate to provide an exception in the criminal context for subsequent disclosure—including by the media. Where a journalist is aware that a Commonwealth officer has disclosed Commonwealth information in breach of the general offence and the journalist knows, intends, or is reckless as to whether, subsequent disclosure will harm, or is reasonably likely to harm, one of the identified public interests, it seems reasonable to impose sanctions in relation to further disclosure of the information.

8.78 As noted above, the Tax Laws Exposure Draft Bill addresses three different situations: the unauthorised disclosure of information by current and former taxation officers; the unauthorised disclosure of information by individuals who receive the information as a result of an unlawful disclosure; and the unauthorised disclosure of information by individuals who receive the information as a result of a lawful disclosure.<sup>66</sup>

---

<sup>65</sup> Ibid.

<sup>66</sup> Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.9].

8.79 In the ALRC's proposed regime, unauthorised disclosure by current and former Commonwealth officers will be covered by the proposed new general secrecy offence, which is intended to apply to all Commonwealth officers, including Commonwealth contracted service providers. Thus, all disclosures between Commonwealth agencies, and between agencies and their contractors, will be covered by the new general secrecy offence and will address the problem identified by John McGinness, above. The proposed subsequent disclosure offence will cover unauthorised disclosure by individuals who receive information as the result of an unlawful disclosure.

8.80 The ALRC is not proposing an offence to cover unauthorised disclosure of information by individuals who receive the information as a result of a lawful disclosure, although the ALRC would be interested in receiving stakeholder views on this issue. Where a Commonwealth officer discloses Commonwealth information with authority to a person or entity that is not a Commonwealth officer—for example, a state or territory public service agency or official, a foreign government or international organisation, or a private sector organisation that is not a contracted service provider—the Commonwealth has the opportunity to ensure that appropriate safeguards are in place, or are put in place, to protect the information. State and territory officers are usually subject to state and territory secrecy provisions,<sup>67</sup> or specific Commonwealth secrecy provisions. The Australian Government can put in place intergovernmental or inter-agency agreements or contractual arrangements with state and territory governments and agencies, foreign governments, and private sector organisations. The equitable action for breach of confidence may also be available in some circumstances.<sup>68</sup>

8.81 The proposed subsequent disclosure offence should be subject to a number of exceptions and defences. It should be subject to an exception where information is legally in the public domain. This exception is discussed in detail in Chapter 9. Other exceptions in the general secrecy offence will also be relevant. For example, where information is disclosed by a Commonwealth officer in the course of his or her functions and duties, or with the authority of an agency head or minister, the information will not have been disclosed in breach of the general secrecy offence and any subsequent disclosure should not, therefore, be an offence under the subsequent disclosure offence.

---

67 State and territory secrecy provisions are discussed in Ch 14.

68 The equitable action for breach of confidence is discussed in Ch 5.

8.82 The proposed subsequent disclosure offence will also be subject to the general defences established by the *Criminal Code*, and discussed in Chapter 9, such as conduct that is justified or excused by or under law,<sup>69</sup> and conduct that is a reasonable response to an emergency, where a person reasonably believes that circumstances of sudden or extraordinary emergency exist; and committing the offence is the only reasonable way to deal with the emergency.<sup>70</sup>

8.83 Chapter 9 also considers the need for comprehensive public interest disclosure legislation. It will be important to ensure that under the proposed regime, where a public interest disclosure is made to a third party in accordance with public interest disclosure legislation, the subsequent disclosure of the information by that third party will not be a criminal offence.

**Proposal 8–3** There should be a new offence in the *Criminal Code* (Cth) (the ‘subsequent disclosure offence’) for subsequent disclosure of Commonwealth information by any person where:

- (a) the information has been disclosed by a Commonwealth officer in breach of the proposed general secrecy offence; and
- (b) the person knows, or is reckless as to whether, the information has been disclosed in breach of the proposed general secrecy offence; and
- (c) the person knows, intends, or is reckless as to whether, the subsequent disclosure of the information will harm, or is reasonably likely to harm, one of the public interests set out in Proposal 7–1.

**Proposal 8–4** The proposed subsequent disclosure offence should include an express exception where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.

## What conduct should be regulated?

8.84 The following section of the chapter considers what conduct should be covered by the proposed general secrecy offence—including unauthorised disclosure, use and receipt of information—and what fault element should attach to that conduct.

8.85 As discussed in Chapter 5, at present, around 60% of Commonwealth secrecy provisions regulate activities other than (but usually in addition to) the disclosure of

---

69        *Criminal Code* (Cth) s 10.5.

70        *Ibid* s 10.3.

information—including soliciting,<sup>71</sup> receiving,<sup>72</sup> obtaining,<sup>73</sup> possessing,<sup>74</sup> making a record of,<sup>75</sup> or using<sup>76</sup> information. Section 70 of the *Crimes Act* regulates publishing or communicating information, and s 79(3) regulates communicating information. The unauthorised disclosure of information is also described in legislation as divulging information.<sup>77</sup>

8.86 The *Criminal Code* contains a number of provisions that extend criminal responsibility in certain circumstances. These provisions regulate: attempt, which must involve conduct that is more than merely preparatory to the commission of the offence;<sup>78</sup> aiding, abetting, counselling or procuring the commission of an offence by another person;<sup>79</sup> incitement, where a person urges the commission of an offence;<sup>80</sup> and conspiracy, where a person conspires with another person to commit an offence punishable by imprisonment for more than 12 months, or by a fine of 200 penalty units or more.<sup>81</sup>

8.87 If a new criminal offence for disclosure of Commonwealth information by Commonwealth officers were included in the *Criminal Code*, as proposed in this Discussion Paper, then these extensions would automatically apply to the offence. The extended criminal liability would catch activity such as soliciting the unauthorised disclosure of Commonwealth information.

8.88 In IP 34, the ALRC asked whether it is appropriate for secrecy provisions to regulate conduct other than the disclosure of information—such as the unauthorised receipt, copying, recording or use of information.<sup>82</sup> The ALRC considers each of these possibilities in the next part of the chapter, and concludes that the general secrecy offence should be limited to the disclosure of Commonwealth information.

## Receiving information

8.89 McGinness argues that provisions that criminalise the mere receipt of information may unduly burden journalists who receive information they have no intention of publishing, or Members of Parliament who are briefed by public servants without authorisation. He notes that s 5 of the *Official Secrets Act 1989* (UK) does not

71 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 165.

72 See, eg, *Crimes Act 1914* (Cth) s 79(6).

73 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 163.

74 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9.

75 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.

76 See, eg, *Aged Care Act 1997* (Cth) s 62-1.

77 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32.

78 *Criminal Code* (Cth) s 11.1.

79 Ibid s 11.2.

80 Ibid s 11.4.

81 Ibid s 11.5.

82 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3-4.

contain offences for mere unlawful possession or receipt of official information.<sup>83</sup> The ALRC's mapping exercise has identified 13 existing secrecy provisions that criminalise the possession or receipt of information.<sup>84</sup>

8.90 The House of Representatives Standing Committee on Legal and Constitutional Affairs also cautioned against the creation of offences prosecuting the mere possession or receipt of confidential information. In the Committee's view, criminal liability should only attach where the person 'has the requisite mental element and proceeds to use, disclose or make a record of the confidential information'.<sup>85</sup>

### ***Submissions and consultations***

8.91 A number of stakeholders expressed concern about provisions that extended to unsolicited possession or receipt of information.<sup>86</sup> The Australian Press Council, for example, submitted that:

The Press Council is of the view that the receipt and holding of information should only be treated as an offence if the recipient has an intention to use the information maliciously, recklessly or with intent to obtain benefit.<sup>87</sup>

8.92 PIAC agreed with McGinness

as to the undesirability of criminalising mere receipt of information where the recipient has no intention of publishing that information. It is important to consider the position of journalists charged in these circumstances, who are faced with the prospect of going to gaol for an indeterminate period of time, rather than breaching their ethical obligations by revealing their sources. There is real potential for such provisions to be used to target end recipients of information, in an effort to pressure them into revealing information that enables 'leaks' to be traced back to their source.<sup>88</sup>

### ***Copying, recording and using information***

8.93 A number of secrecy provisions regulate conduct potentially leading up to an unauthorised disclosure of information, such as copying and recording of information, as well as unauthorised use of information. The Privacy Commissioner has drawn a distinction between the use of information and the disclosure of information on the basis that, in general terms, a 'use' refers to the handling of information within an

83 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 85. See also Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), [232]–[233].

84 See eg *Crimes Act 1914* (Cth) ss 79(4)–(6), 83; *Defence (Special Undertakings) Act 1952* (Cth) s 9(2).

85 Australian Parliament—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), [7.11.7].

86 Law Council of Australia, *Submission SR 30*, 27 February 2009; The Treasury, *Submission SR 22*, 19 February 2009.

87 Australian Press Council, *Submission SR 16*, 18 February 2009.

88 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

organisation; while a ‘disclosure’ refers to the release of information to those outside an organisation.<sup>89</sup>

8.94 The Tax Laws Exposure Draft Bill covers both recording and disclosure of taxpayer information.<sup>90</sup> The Explanatory Material accompanying the Draft Bill states that the former conduct is covered ‘not only to ensure that information is not disclosed unlawfully, but that the information is not recorded in another form that can be readily accessed by others’.<sup>91</sup>

#### **Submissions and consultations**

8.95 A number of stakeholders submitted that conduct other than disclosure should be regulated in some way. The ATO submitted that the primary mischief addressed by the operation of tax secrecy provisions is disclosure, but noted that the unauthorised collection, use and recording of information could lead to inadvertent disclosures of information. Tax law also regulates access to information—for example, s 8XA of the *Taxation Administration Act* prohibits unauthorised access to information about another person’s tax affairs. The ATO stated that access to, use, recording and disclosure of information should be addressed, but noted that such provisions should be separate from secrecy provisions.<sup>92</sup>

8.96 In its submission, the Department of Education, Employment and Workplace Relations (DEEWR) noted that the primary reason to have secrecy provisions was to prevent the harm that may flow from disclosure:

This reason for protecting information against unauthorised disclosure would seem to apply equally to ensuring that the collection and use of the information was also appropriate. For example, accessing a departmental database would generally be considered a ‘use’ of the information. If a staff member was to intentionally access a database to locate a spouse, who purposely did not want to be found because of domestic violence issues, then the harm that could flow from this could be significant. It would seem equally desirable and necessary to regulate this behaviour as it would the inappropriate disclosure of information.<sup>93</sup>

8.97 The AIC noted that the espionage offences in s 79 of the *Crimes Act*—which apply to unauthorised communication of information—also apply to unauthorised retention or receipt of information; failure to comply with a reasonable direction to dispose of information; and failure to take reasonable care of information. Section 91.1 of the *Criminal Code* also applies to unauthorised making, obtaining or copying a

---

89 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), NPP 2.

90 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 3 pt 1 s 355-20.

91 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.15].

92 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

93 Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

record. The AIC considers it essential to preserve these elements in the intelligence context.<sup>94</sup>

### **Disclosing, divulging, communicating**

8.98 As noted above, most secrecy provisions regulate the disclosure of information, although this is described in different ways, including divulging, communicating and publishing information.

#### ***Submissions and consultations***

8.99 The ATO and APRA submitted that disclosure should be the primary mischief addressed by secrecy provisions.<sup>95</sup> Ron Fraser expressed the view that:

Much of the conduct covered by many secrecy provisions, such as receipt, collection, use or recording or otherwise dealing with information ... seems marginal to the real concerns of disclosure and or communication.<sup>96</sup>

8.100 The DHS noted that while there are arguments in favour of including other activity such as unauthorised collection, accessing, browsing, use or disclosure,

it can be argued that the prohibition in secrecy provisions should be limited to use and disclosure, or even disclosure alone. Disclosure is the dealing most likely to lead to disadvantage to the person concerned.<sup>97</sup>

8.101 The DHS also noted the legal issues that arise as a consequence of the inconsistent terminology used in legislation:

For example, Medicare Australia officers are variously forbidden from ‘divulging or communicating’ (*National Health Act*, *Health Insurance Act*), ‘disclosing or producing’ (*Medical Indemnity Act*), and ‘disclosing’ only (*Aged Care Act*, *Dental Benefits Act*). There is a difference between ‘divulging or communicating’ (Medicare Australia—*Health Insurance Act*, *National Health Act*) and ‘disclosing’ (Centrelink and Australian Hearing) as it is possible to divulge or communicate information which has already been disclosed and is publicly known. Meanwhile [Child Support Agency] officers are forbidden from ‘communicating’ only and [Commonwealth Rehabilitation Service] Australia from ‘divulging’ only. The rationale for these distinctions is not clear and does not easily justify the withholding of information which another agency has already properly disclosed publicly.<sup>98</sup>

---

94 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

95 Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

96 R Fraser, *Submission SR 42*, 23 March 2009.

97 Department of Human Services, *Submission SR 26*, 20 February 2009.

98 Ibid.

8.102 The Law Council of Australia expressed some concern over the use of the word ‘publish’ in s 70 of the *Crimes Act*, noting that, in the absence of a definition, ‘guidance as to the meaning of the term may need to be taken from case law, including defamation law, which may not be appropriate for cases dealing with secrecy’.<sup>99</sup>

8.103 The AGD stated that:

The conduct that should be regulated by secrecy provisions will depend upon the policy rationale and harm sought to be avoided. If harm can be caused by unauthorised handling, access or use of information, then it would seem appropriate for these actions to also be prohibited.<sup>100</sup>

### ALRC’s views

8.104 The ALRC agrees with the AGD that the focus of the proposed new general secrecy offence should be the potential harm caused by the conduct. In this case, the ALRC’s view is that the relevant harm to the public interests identified in Chapter 7 would come from unauthorised disclosure of Commonwealth information and that this should be the focus of the proposed general secrecy offence. The term ‘disclosure’ is preferred because it is widely used and understood in the privacy context. The provisions of the *Criminal Code* dealing with extension of criminal responsibility will ensure that a range of other activity leading up to an unauthorised disclosure, such as procuring or conspiring to bring about a disclosure, may also attract criminal sanctions.

8.105 While the ALRC proposes that the new general secrecy offence be limited to ‘disclosure’ of Commonwealth information, in some specific contexts it will be appropriate to regulate other activity. For example, in Chapter 10, the ALRC discusses the need for a wider range of activity to be regulated in the intelligence context. The ALRC can also see merit in restricting an officer’s access to certain information in some contexts; for example, the prohibition on browsing in the tax context. But these are context-specific requirements and would not fit comfortably into a general provision applying to all Commonwealth officers and all Commonwealth information.

8.106 The ALRC agrees with the majority of stakeholders that the mere receipt of information should not be covered in the general secrecy offence. As discussed above, however, the ALRC considers that certain subsequent disclosures of information by a person who knows, or is reckless as to whether, the information has been disclosed in breach of the general secrecy offence, should also be a criminal offence in some circumstances.<sup>101</sup>

8.107 How information is ‘used’ within an agency is a different and wider issue than simply protecting the information from unauthorised disclosure. A clear distinction is drawn in the Privacy Commissioner’s guidelines, discussed above, between use and

---

99 Law Council of Australia, *Submission SR 30*, 27 February 2009.

100 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

101 Proposal 8–3.

disclosure. While it may be necessary to criminalise inappropriate uses in some circumstances—for example, where information is security classified or otherwise sensitive—this is an issue that requires consideration on an agency by agency basis and not one that can be addressed in a general secrecy offence.

8.108 The ALRC’s view is that a great deal of conduct that may precede an unauthorised disclosure, such as recording or copying information, could be dealt with through administrative procedures and penalties. In particular, the example provided in the Explanatory Material to the Tax Laws Exposure Draft Bill of an officer copying a person’s tax information into her diary, where the conduct is discovered before any disclosure has occurred, would appear to be of this order. Such conduct may attract criminal penalties, in more serious circumstances, under the *Criminal Code* provisions extending criminal responsibility, for example, where copying the information provides evidence of complicity or conspiracy.

### **Fault element attaching to disclosure**

8.109 The *Criminal Code* provides that fault elements may include intention, knowledge, recklessness or negligence, but that particular offences may specify other fault elements.<sup>102</sup> As noted in Chapter 5, under the *Code*, if the legislation creating an offence does not specify a fault element for a physical element consisting of conduct, the fault element is intention.<sup>103</sup> Where an offence provision does not specify a fault element for a physical element consisting of a circumstance or a result, the fault element is recklessness.<sup>104</sup>

8.110 The ALRC’s mapping exercise indicates that the majority of Commonwealth secrecy provisions do not stipulate fault elements. This is also true of s 70 of the *Crimes Act*. On the basis of the provisions of the *Criminal Code*, noted above and discussed further in Chapter 5, and given the serious nature of the offence, the fault element attaching to the conduct of publishing or communicating information under s 70 of the *Crimes Act* is intention. The ALRC proposes that the fault element attaching to the conduct of disclosure in the proposed new general secrecy offence should also be intention.

8.111 There is, however, a question of whether the proposed provision should include recklessness as a fault element attaching to disclosure. Section 5.4 of the *Criminal Code* provides that:

- (1) A person is reckless with respect to a circumstance if:

---

102 *Criminal Code* (Cth) s 5.1. For example, the *Criminal Code* itself stipulates an additional fault element of ‘dishonesty’ in relation to offences in Ch 7—*The Proper Administration of Government*. Dishonesty is defined as ‘dishonest according to the standards of ordinary people’ and ‘known by the defendant to be dishonest according to the standards of ordinary people’: s 130.3.

103 *Ibid* s 5.6(1).

104 *Ibid* s 5.6(2).

- (a) he or she is aware of a substantial risk that the circumstance exists or will exist; and
  - (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
- (2) A person is reckless with respect to a result if:
- (a) he or she is aware of a substantial risk that the result will occur; and
  - (b) having regard to the circumstances known to him or her, it is unjustifiable to take the risk.
- (3) The question whether taking a risk is unjustifiable is one of fact.
- (4) If recklessness is a fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.

8.112 The ALRC has identified a number of secrecy provisions in which the fault element attaching to disclosure is recklessness. For example, s 23YO(1) of the *Crimes Act* provides:

A person is guilty of an offence if:

- (a) the person has access to any information stored on the Commonwealth DNA database system or [National Criminal Investigation DNA Database] or to any other information revealed by a forensic procedure carried out on a suspect, offender or volunteer; and
- (b) the person's conduct causes the disclosure of information other than as provided by this section; and
- (c) the person is reckless as to any such disclosure.<sup>105</sup>

8.113 As the proposed general secrecy offence requires that there be harm to significant public interests, a reasonable likelihood of harm, or an intention to harm those interests, the ALRC would be interested in stakeholder views on whether it would be appropriate to include recklessness as to disclosure as part of the offence. This would mean that where a Commonwealth officer was aware of a substantial risk that disclosure would occur and, having regard to the circumstances, it was unjustifiable to take the risk, he or she took the risk.

**Proposal 8–5** The proposed general secrecy offence should regulate the disclosure of Commonwealth information. The fault element attaching to disclosure should be intention.

105 See also *Crimes Act 1914* (Cth) s 3ZQJ.

## **What information should be protected?**

8.114 In Chapter 5, the ALRC considers the various categories of information protected by the hundreds of existing secrecy provisions in federal legislation.<sup>106</sup> In this section, the ALRC considers what information should be protected by the proposed new general secrecy offence.

8.115 The *Australian Government Protective Security Manual* (PSM)<sup>107</sup> binds all Commonwealth agencies to a series of procedures designed to protect Commonwealth information, including classified and other sensitive information. The PSM refers to ‘official information’, which includes any information received or collected by, or on behalf of, the Government, through its agencies and contractors.<sup>108</sup> Section 70 of the *Crimes Act* applies to any current and former Commonwealth officer who publishes or communicates ‘any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer’. This would include official information received or collected by the Australian Government, as well as information generated within Government.

8.116 Regulation 2.1 of the *Public Service Regulations* also applies broadly to ‘information which the APS employee obtains or generates in connection with the APS employee’s employment’.

8.117 Other possible models include s 142.2 of the *Criminal Code*, which prohibits a ‘Commonwealth public official’ from dishonestly using information ‘obtained in the official’s capacity as a Commonwealth public official’. Section 18(2) of the *Australian Security Intelligence Organisation Act 1979* (Cth) (the ASIO Act) applies to ‘any information or matter that has come to the knowledge or into the possession of the person by reason of his or her being, or having been, an officer or employee of the Organisation’.

8.118 The Explanatory Material that accompanies the Tax Laws Exposure Draft Bill states that:

Protected information includes information in the form of written documents, conversations, electronic recordings, transcripts or any other form in which information can be recorded. It includes information obtained directly from a taxpayer or information generated by the ATO (for instance, through the collating, cross referencing or summarising of related information from a variety of different sources).<sup>109</sup>

---

106 See also Ch 10.

107 Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM)* (2005).

108 *Ibid*, pt C, [1.3].

109 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [2.17].

### ALRC's views

8.119 The ALRC proposes to retain a broad definition of Commonwealth information in the proposed new general secrecy offence. The provision is intended to be an umbrella provision of general application applying to all Commonwealth officers and to all Commonwealth information. It is intended to address gaps left by more specific provisions that are limited in their scope to particular parties or particular information. However, the scope of the provision will be narrowed by the requirement to prove that the disclosure of the information caused harm, was reasonably likely to cause harm, or was intended to cause harm, as discussed in Chapter 7.

8.120 For the reasons set out in Chapter 13, the ALRC is of the view that the language currently used in reg 2.1 of the *Public Service Regulations* to describe the information covered by the regulation is too wide. In that chapter, the ALRC proposes that the language in reg 2.1 should be amended to specify ‘information to which an APS employee has access by reason of his or her being an APS employee’ in order to bring the regulation more into line with the proposed new general secrecy offence and also because, in the ALRC’s view, the phrase ‘in connection with’ currently used in the regulation is too broad.<sup>110</sup>

8.121 The formulation used in the *Criminal Code* noted above—that is, information obtained in the official’s capacity as a Commonwealth public official—appears to be too narrow for the purposes of the general secrecy offence. This formulation limits the relevant information to that which a Commonwealth public official has legitimate access to in his or her formal capacity. In a provision dealing with unauthorised disclosure, it is important to include information that a Commonwealth officer may have access to because of his or her position, whether or not that access is legitimate. This would include, for example, Commonwealth information that the officer accessed in contravention of agency guidelines or rules. This information may not have been available to the particular officer in his or her formal capacity as a Commonwealth officer because, for example, he or she may not have had an adequate security clearance.

8.122 The approach adopted in s 70 of the *Crimes Act* and s 18(2) of the ASIO Act is not limited in this way. These provisions apply to any information the officer may access by virtue of being, or by reason of being, an officer. This would include information that a person is able to access because of his or her position, despite access being in breach of agency rules.

---

110 Proposal 13–1.

8.123 The ALRC prefers the term ‘information’ to the *Crimes Act* formulation of ‘any fact or document’. As indicated in the Explanatory Material to the Tax Laws Exposure Draft Bill, ‘information’ can be given a wide meaning to include information in oral, written, electronic or any other form. Much information intended to be covered by the proposed general offence will not be factual or in documentary form, although the ALRC notes that the term ‘document’ is defined widely in s 25 of the *Acts Interpretation Act 1901* (Cth). The ALRC proposes that the general secrecy offence apply to ‘any information to which a person has, or had, access by reason of his or her being, or having been, a Commonwealth officer’.

**Proposal 8–6** The proposed general secrecy offence should apply to any information to which a person has, or had, access by reason of his or her being, or having been, a Commonwealth officer as defined in Proposal 8–1.

## **9. General Secrecy Offence: Exceptions and Penalties**

---

### **Contents**

Exceptions and defences	293
Introduction	293
Exceptions versus defences	294
Defences available under the <i>Criminal Code</i>	294
Exceptions and defences for inclusion in the general secrecy offence	295
In the course of an officer's functions and duties	297
Required or authorised by or under law	300
On the authority of specified persons	302
To specified persons or entities	303
For the purposes of law enforcement	304
For use in legal proceedings	307
With consent	308
A serious threat to a person's life, health or safety	309
A serious threat to public health or public safety	312
Information already in the public domain	312
Public interest disclosure	315
Submissions and consultations	320
ALRC's views	321
Penalties	324
Penalties in existing secrecy provisions	325
Submissions and consultations	326
ALRC's views	327
Penalties for subsequent disclosure	330
Other issues	333
Consent of the Attorney-General	333
Infringement notices	336
Injunctions	338

### **Exceptions and defences**

#### **Introduction**

9.1 Commonwealth secrecy offences include a range of exceptions and defences—for example, disclosure in the course of an officer's duties, or for the purposes of the relevant Act, or disclosure of information that is already in the public domain.

Protection from criminal liability under secrecy offences may also arise as a result of public interest disclosure (or ‘whistleblower’) legislation. This chapter will consider which exceptions or defences should be included in the proposed new general secrecy offence, and the proposal for public interest disclosure legislation discussed in the recent House of Representatives Standing Committee on Legal and Constitutional Affairs report.<sup>1</sup>

### **Exceptions versus defences**

9.2 A distinction may be drawn between an ‘exception’, which limits the scope of conduct prohibited by a secrecy offence, and a ‘defence’, which may be relied on by a person whose conduct is prohibited by a secrecy offence.

9.3 Section 94 of the *Australian Trade Commission Act 1985* (Cth) provides an example of an ‘exception’, stating that ‘a person to whom this section applies shall not, either directly or indirectly, except for the purposes of this Act’ disclose any information concerning the affairs of another person acquired by reason of the person’s employment. Section 191(2A) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth), on the other hand, provides that ‘it is a defence to a prosecution’ for disclosing information if the information relates to a loan made by Indigenous Business Australia and the information was communicated to a person authorised in writing, by the person to whose affairs the document relates, to receive the information.

9.4 The Australian Government Attorney-General’s Department (AGD) *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers (Guide to Framing Commonwealth Offences)* makes clear the practical consequences of providing one or the other:

In general, the prosecution should be required to prove all aspects of a criminal offence beyond reasonable doubt. A matter should be included in a defence, thereby placing the onus on the defendant, only where the matter is peculiarly within the knowledge of the defendant; and is significantly more difficult and costly for the prosecution to disprove than for the defendant to establish.<sup>2</sup>

9.5 The Guide goes on to state that the fact that it is difficult for the prosecution to prove an element of an offence has not traditionally been considered, in itself, a sound justification for taking the significant step of reversing the onus of proof.

### **Defences available under the *Criminal Code***

9.6 The *Criminal Code* (Cth) sets out a range of circumstances in which a person is not criminally responsible for an offence. For ease of reference, the ALRC has referred

---

1 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

2 Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 28–29.

to these as ‘defences’, although the *Code* does not characterise them in this way.<sup>3</sup> Even where a secrecy offence does not contain any express exceptions or defences, these *Code* defences may nevertheless be available. The *Code* includes the following defences of general application, that may be relevant in the context of the general secrecy offence:

- mistake or ignorance of fact—which applies where the fault element is something other than negligence (s 9.1);
- mistake of fact—which applies where the offence is one of strict liability (s 9.2);
- duress (s 10.2);
- sudden or extraordinary emergency (s 10.3); and
- conduct justified or excused by or under a law (s 10.5).

9.7 In its submission, the AGD noted that the *Code* provisions were intended to codify the general defences available at common law.<sup>4</sup> The *Guide to Framing Commonwealth Offences* states that these defences are of general application to Commonwealth offences, and that defences covering the same matters should not be included in individual offences.<sup>5</sup>

## Exceptions and defences for inclusion in the general secrecy offence

9.8 Chapter 5 identifies a range of exceptions and defences found in existing secrecy provisions. These include where information is disclosed:

- in the course of a person’s functions and duties as an officer or an employee;
- as required or authorised by or under law;
- on the authority of specified persons;
- to specified persons or entities;
- for the purposes of law enforcement;

<sup>3</sup> Part 2.3 of the *Criminal Code* (Cth) is headed ‘Circumstances in which there is no criminal responsibility’.

<sup>4</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

<sup>5</sup> Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 27.

- for use in legal proceedings;
- with the consent of the person or entity to whom the information relates;
- to avert serious threats to a person's life or health; and
- in the public or national interest.

9.9 In the Issues Paper, *Review of Secrecy Laws* (IP 34) the ALRC asked which exceptions should be included in the general secrecy offence.<sup>6</sup> In particular, the ALRC asked whether the first six exceptions listed above should be included, and whether there were any others that should be included.<sup>7</sup>

#### ***Submissions and consultations***

9.10 The Public Interest Advocacy Centre (PIAC) submitted that the first six exceptions listed above were likely to be of such frequent and general application that they should be included in all secrecy provisions.<sup>8</sup> The Australian Prudential Regulation Authority (APRA) noted that these elements essentially reflected the structure of the secrecy provision in the *Australian Prudential Regulation Authority Act 1998* (Cth).<sup>9</sup> APRA's view was that these exceptions worked well in the regulatory context where it is essential for regulators to be able to exchange information with other regulators, to brief the executive government, and to use information in legal proceedings.<sup>10</sup>

9.11 The AGD suggested the following exceptions and defences should be included in the general secrecy offence: disclosure in the course of an individual's duties; disclosure in accordance with the law; disclosure where the information has been made lawfully available to the public; disclosure authorised by an agency head; and disclosure to prevent a serious and imminent threat to life or health.<sup>11</sup>

9.12 In this chapter, the ALRC considers the suggested exceptions and defences and whether each should be included in the proposed general secrecy offence. The ALRC proposes that there should be three express exceptions included in the offence provision, and examines how the defences in the *Criminal Code* would operate in relation to the offence.

---

<sup>6</sup> Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 4–1.

<sup>7</sup> Ibid, Question 4–2.

<sup>8</sup> Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

<sup>9</sup> Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009; *Australian Prudential Regulation Authority Act 1998* (Cth) s 56.

<sup>10</sup> Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

<sup>11</sup> Attorney-General's Department, *Submission SR 36*, 6 March 2009.

### In the course of an officer's functions and duties

9.13 Secrecy provisions commonly allow information to be disclosed in the performance of a person's functions and duties as an employee or officer. For example, the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) provides that secrecy provisions do not extend to a person handling information 'in the performance of the person's functions or duties' under the Act.<sup>12</sup>

9.14 A 2006 Treasury review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review) noted, however, that the meaning of disclosure in the 'course of duties of an officer' is uncertain and should be clarified.<sup>13</sup> The Explanatory Material to the Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) (the Tax Laws Exposure Draft Bill) notes that:

Specific disclosures for taxation officers are found across the taxation laws. These generally provide for disclosures to be made by the Australian Taxation Office (ATO) to another Government agency in circumstances in which taxpayer information will be used to enable that other agency to fulfil some aspect of its function more effectively.<sup>14</sup>

9.15 The Tax Laws Exposure Draft Bill, like a number of existing secrecy provisions, attempts to clarify some of the ambiguities by providing a non-exhaustive list of disclosures that fall within the 'performance of duties' exception.<sup>15</sup> Some of these are quite general—for example, 'for the purpose of administering a taxation law',<sup>16</sup> or 'for the purpose of criminal, civil or administrative proceedings (including merits review or judicial review) that are related to a taxation law'.<sup>17</sup> Some are more specific—for example, 'for the purpose of determining whether to make an ex gratia payment; or administering such a payment; in connection with administering a taxation law'.<sup>18</sup>

9.16 In IP 34, the ALRC asked in what circumstances Commonwealth secrecy laws should permit the disclosure of Commonwealth information in the performance of a Commonwealth officer's functions and duties.<sup>19</sup>

### Submissions and consultations

9.17 A number of stakeholders, including the Australian Securities and Investments Commission (ASIC), APRA, the Australian Bureau of Statistics (ABS) and the ATO,

12     *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2).

13     The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 19.

14     Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.6].

15     Ibid, [5.8].

16     Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 subsection 355-45(2) table item 1.

17     Ibid sch 1 item 1 subsection 355-45(2) table item 3.

18     Ibid sch 1 item 5.

19     Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 4-2(a).

noted that the secrecy provisions regulating their activity were in the form of a general prohibition on disclosure, followed by a list of situations in which disclosure is authorised.<sup>20</sup>

9.18 ASIC submitted that the specific circumstances in which disclosures should be permitted must be determined by reference to the functions that are performed and the duties that are exercised by each Commonwealth agency. ASIC noted that where secrecy provisions attempt to list authorised disclosures—as in s 127 of the *Australian Securities and Investments Commission Act 2001* (Cth) (the ASIC Act)—it is important to ensure that the list is inclusive, rather than exhaustive and suggested that s 127 of the ASIC Act may be an appropriate model.<sup>21</sup>

9.19 Section 127 provides a detailed list of situations in which disclosure is specifically authorised—for example, to the Minister, to APRA or to a Royal Commission; but also includes more open ended elements—for example, s 127(3) provides that a disclosure is authorised where it is for the purposes of performing functions as a member, a staff member or an ASIC delegate.

9.20 The ATO also expressed support for the proposition that secrecy provisions should list those disclosures that are permitted to be made to specific agencies for specific purposes, as well as a general exception permitting disclosures in the performance of an officer's duties. The ATO considered this last exception to be fundamental to the proper functioning of the taxation system:

The performance of duties exception is flexible enough to allow disclosures of information which may not arise directly under a taxation law, but which relate to the ATO's administration of taxation laws. For example, it allows disclosures for the purpose of complying with equitable, common law and statutory obligations, such as responding to a request for a statement of reasons under the *Administrative Decisions (Judicial Review) Act 1977*, and producing information in response to certain court orders. The ATO considers that the flexibility of this exception is integral to allowing the ATO to comply with these broader legislative, equitable and common law obligations.<sup>22</sup>

9.21 The Treasury also expressed support for a 'performance of duty' exception, on the basis that there is existing jurisprudence around the scope of the term.<sup>23</sup> While agreeing that there is a considerable body of case law around the term 'in the performance of duties', the Department of Human Services (DHS) noted that its meaning remained vexed.<sup>24</sup>

---

20 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

21 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

22 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

23 The Treasury, *Submission SR 22*, 19 February 2009.

24 Department of Human Services, *Submission SR 26*, 20 February 2009.

9.22 The AGD suggested that, in addition to legislative lists of authorised disclosures,

Memorandums of understanding (MOU) or internal guidelines may also be used to set out circumstances when information can be disclosed from one agency to another. This may provide a more flexible approach, as the detail of information sharing arrangements can be left to documents more easily amended.<sup>25</sup>

9.23 Ron Fraser stated that:

In effect, the exceptions to a number of secrecy provisions (eg in the *National Health Act 1953* and the *Health Insurance Act 1973*) operate as guidelines to the agency as to appropriate disclosures of information: they don't need to be appended to a criminal provision. These rules relating to release, other than under an FOI request, have become an internalised part of the culture of an agency and its officers with little or no reference to the underlying criminal penalties.<sup>26</sup>

#### ***ALRC's views***

9.24 In the ALRC's view, it would be important to include an exception in the general secrecy offence for disclosure in the course of an officer's functions or duties. However, in the proposed new general secrecy offence it will not be possible to include a comprehensive list of those disclosures that fall within this exception, because the provision is intended to apply across all agencies and all Commonwealth information. It should be possible to provide clarity about the scope of the exception in other ways.

9.25 The legislation regulating some specific agencies, such as the ATO and ASIC, includes a list of authorised disclosures, which are indicative of what falls within an officer's duties or functions in those agencies. Such disclosures would fall within the 'duties and functions' exception to the proposed general secrecy offence.<sup>27</sup>

9.26 It also would be possible to indicate those disclosures that fall within an officer's functions and duties by issuing agency guidelines or inter-agency memorandums of understanding (MOUs). In some cases, and in relation to some agencies, this will not be necessary, but where there is doubt about the scope of an officer's duties these mechanisms may prove helpful.

9.27 In relation to a number of existing secrecy provisions that set up a general prohibition on disclosure and then proceed to list exceptions to the prohibition, it may be possible to do away with the prohibition—while leaving the list of authorised disclosures in place—and rely, instead, on the proposed general secrecy offence.

---

25 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

26 R Fraser, *Submission SR 42*, 23 March 2009.

27 Such disclosures may also fall within the 'conduct justified or excused by or under law' exception, discussed below.

### **Required or authorised by or under law**

9.28 Secrecy provisions commonly provide that information may be disclosed ‘for the purposes of this Act’.<sup>28</sup> It is also common for secrecy provisions to permit disclosure for the purposes of other legislation,<sup>29</sup> or intergovernmental arrangements.<sup>30</sup> As discussed above, many secrecy provisions also include a list of specifically authorised disclosures.

9.29 The *Criminal Code* includes a defence of ‘lawful authority’ where ‘the conduct constituting the offence is justified or excused by or under a law’.<sup>31</sup> The *Commonwealth Criminal Code: Guide for Practitioners* states that this provision:

Provide[s] a general defence which will excuse or justify conduct which is authorised by law. The law in question must be a law of the Commonwealth ... The reference to conduct which is justified or excused ‘by or under a law’ recognises that the authorisation may be indirect or implied, rather than explicit.<sup>32</sup>

9.30 The *Code* defence will protect disclosures in a range of circumstances, including those made in accordance with provisions that:

- expressly allow disclosures to particular persons or agencies—such as s 127 of the ASIC Act discussed above;
- allow disclosure ‘for the purposes of the Act’—such as s 3C(2A) of the Taxation Administration Act 1953 (Cth); and
- allow disclosure for the purposes of another Act—such as s 79A(2) of the *Reserve Bank Act 1959* (Cth), which permits disclosure for the purposes of that Act and certain other Acts including the *Banking Act 1959* (Cth), *Corporations Act 2001* (Cth), *Payment Systems (Regulation) Act 1998* (Cth) and *Payment Systems and Netting Act 1998* (Cth).

### ***Submissions and consultations***

9.31 The Treasury submission queried whether there was a meaningful distinction between a ‘performance of duties’ exception and disclosures that are allowed ‘for the

---

28 See eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 65(4); *Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992* (Cth) s 14(3A); *Taxation Administration Act 1953* (Cth) s 3C(2A).

29 See, eg, *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 49(3); *Reserve Bank Act 1959* (Cth) s 79A(2).

30 See, eg, *Disability Discrimination Act 1992* (Cth) s 127(3).

31 *Criminal Code* (Cth) s 10.5.

32 Australian Government Attorney-General’s Department and the Australian Institute of Judicial Administration, *The Commonwealth Criminal Code: A Guide for Practitioners* (2002), 233.

purposes of an Act'. A disclosure for the purposes of the regulating legislation is likely to fall within the duties of an officer.<sup>33</sup>

9.32 The Commonwealth Director of Public Prosecutions (CDPP) noted that because the defence of lawful authority in s 10.5 of the *Criminal Code* is of general application, it is not necessary to duplicate the defence in other legislation containing secrecy provisions.<sup>34</sup>

9.33 Liberty Victoria submitted that individuals authorised to disclose information under the FOI Act should not be penalised for doing so, and noted that this was so under the Act, if the information was released in good faith.<sup>35</sup>

#### *ALRC's views*

9.34 The ALRC notes that, given the general application of the defence of lawful authority under the *Criminal Code*, it is not necessary to expressly include this defence in the proposed general secrecy offence. In Chapter 15, the ALRC proposes that Australian Government agencies should develop and implement policies clarifying the application of relevant secrecy laws to their information holdings, including the circumstances in which the unauthorised handling of information could lead to criminal proceedings.<sup>36</sup> It would be helpful to include a reference in any such policy to the 'lawful authority' defence.

9.35 In addition, the ALRC proposes that Australian Government agencies should develop and administer training and development programs for their employees, about the information-handling obligations relevant to their position. Any such training and development should allude to the obligations imposed by the proposed general criminal offence and relevant exceptions and defences, including 'lawful authority'.<sup>37</sup>

9.36 Finally, the ALRC proposes that private sector organisations that perform services for or on behalf of the Australian Government under contract should take steps to ensure that all employees who access Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal, civil or administrative liability could result.<sup>38</sup> This should include reference to the obligations imposed by the proposed general criminal offence and relevant exceptions and defences, including 'lawful authority'.

---

33 The Treasury, *Submission SR 22*, 19 February 2009.

34 Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

35 Liberty Victoria, *Submission SR 19*, 18 February 2009.

36 Proposal 15–1.

37 Proposal 15–4.

38 Proposal 15–7.

### **On the authority of specified persons**

9.37 Chapter 5 considers a range of secrecy provisions that allow disclosure of information at the discretion and with the authority of specified office-holders, such as the Commissioner of Taxation,<sup>39</sup> or other persons, including agency heads<sup>40</sup> or the responsible Minister.<sup>41</sup> A number of these provisions require the authorising person to certify that the disclosure is necessary in the public interest.

9.38 For example, s 86–3 of the *Aged Care Act 1997* (Cth) provides that the Secretary of the Department of Health and Ageing may disclose protected information in a range of circumstances including ‘if the Secretary certifies, in writing, that it is necessary in the public interest to do so in a particular case—to such people and for such purposes as the Secretary determines’. Section 130(3) of the *Health Insurance Act 1973* (Cth) provides that the agency head may disclose information where the Minister certifies, by instrument in writing, that disclosure is necessary in the public interest.<sup>42</sup>

### **Submissions and consultations**

9.39 The ATO submitted that it would not be appropriate for disclosures of taxpayer information to be made on the authority of specified persons. In the ATO’s view, such discretionary authority would provide less certainty for tax officers and taxpayers.<sup>43</sup>

9.40 The Treasury also expressed the view that:

It is important for the legislature to turn its mind to the particular instances where it considers a disclosure is warranted. Therefore, Treasury does not support broad provisions permitting disclosures when authorised by some authority.<sup>44</sup>

9.41 On the other hand, the AGD stated that, while completely codifying the circumstances in which disclosure is allowed provides clarity and certainty for officers, this approach may prove to be insufficiently flexible:

Including a provision to enable the agency head or other senior officers to authorise disclosure may provide greater flexibility as it may enable disclosure in new or unforeseen circumstances. It also provides a level of accountability by requiring a senior officer to consider whether disclosure would be consistent with policy considerations in a particular case.<sup>45</sup>

---

39     *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C(5)(b).

40     See, eg, *Customs Administration Act 1985* (Cth) s 16(3).

41     See, eg, *Health Insurance Act 1973* (Cth) s 130(3).

42     See also *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 209; *Ombudsman Act 1976* (Cth) s 35A.

43     Australian Taxation Office, *Submission SR 13*, 16 February 2009.

44     The Treasury, *Submission SR 22*, 19 February 2009.

45     Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

***ALRC's views***

9.42 In Chapter 7, the ALRC proposes that the new general secrecy offence apply to those disclosures of Commonwealth information that harm, are reasonably likely to harm, or are intended to harm specified public interests. In Chapter 8, the ALRC proposes that the offence bind agency heads, as well as ministers. It is possible that, in some circumstances, it will be in the overall public interest to disclose information, despite the fact that the information may harm one of the specified public interests. For example, although the public disclosure of certain information is likely to harm Australia's relations with a particular country—that is, it is reasonably likely to harm the international relations of the Commonwealth—the responsible minister may be of the view that it is in the overall public interest to disclose the information.

9.43 In addition, it may be necessary for an officer to disclose information in unforeseen circumstances where the disclosure does not fall clearly within the officer's duties or functions. The ALRC notes the advice of the AGD that, in such circumstances, a level of flexibility is necessary. Because the information protected by the proposed general secrecy offence has the potential to harm the public interests specified in Chapter 7, the ALRC's view is that, where disclosure of the information does not fall clearly within an officer's functions or duties, he or she should be required to seek authority for the disclosure from the agency head or the minister. Where harm is likely to be caused to the specified public interests by the disclosure of information, the competing public interests should be considered at a senior level.

9.44 The ALRC proposes, therefore, that the general secrecy offence include an exception for disclosure of information, where the disclosure has been authorised by the relevant agency head or minister, and the agency head or minister certifies that the disclosure is in the public interest.

**To specified persons or entities**

9.45 As discussed in Chapter 5, a number of secrecy provisions provide exceptions to allow disclosures to specified persons or entities, such as ministers or government agencies.<sup>46</sup> These provisions are aimed at facilitating the legitimate sharing of information within government.

9.46 In other circumstances, provisions provide that information must not be disclosed to specified persons—for example, the minister. The Explanatory Material to the Tax Laws Exposure Draft Bill states that information may only be disclosed to ministers where this is specifically provided for in the legislation:

As with the current law, this recognises the importance of a separation between the Executive and Legislative arms of government and the administration of the taxation

---

46 See, eg, *Environment Protection (Alligator Rivers Region) Act 1978* (Cth) s 31.

laws and sensitivities associated with the possible release of taxpayer information into a public forum.<sup>47</sup>

9.47 It would not be an offence, however, under the Tax Laws Exposure Draft Bill for a taxation officer to provide taxpayer information to a minister for the purpose of enabling a minister to exercise a power or perform a function under a taxation law.<sup>48</sup>

### ***Submissions and consultations***

9.48 A number of submissions—discussed above in relation to the exception for disclosure in the course of an officer’s functions and duties—expressed support for provisions that include a list of authorised disclosures to specified persons or entities. In its submission, the AGD noted that:

Secrecy provisions that contain specific provisions about disclosure to Ministers are generally only found in confidentiality provisions relating to information collected by government agencies for service delivery purposes. In these cases, such information may not, as a general rule, need to be provided to Ministers unless the Minister has a particular role in the relevant decision-making process.<sup>49</sup>

### ***ALRC’s views***

9.49 The ALRC is not proposing to include exceptions in the general secrecy offence to allow disclosure to ministers or to other specified persons or entities. These matters need to be considered at an individual agency level. Any disclosure to a minister or other specific person or entity that has been authorised, for example, in legislation, through agency guidelines, or inter-agency MOUs will fall within the exception for disclosures in the course of an officer’s functions or duties, or with the authority of the agency head.

9.50 Where it is necessary to restrict disclosure of certain Commonwealth information to a minister, or other specified persons or entities, a specific secrecy provision can be used.

### **For the purposes of law enforcement**

9.51 As discussed in Chapter 5, a number of secrecy provisions expressly provide exceptions for the disclosure of information for various law enforcement and investigatory purposes. For example, s 86–3 of the *Aged Care Act* provides that the Secretary may disclose protected information in a range of circumstances including:

if the Secretary believes, on reasonable grounds, that disclosure of the information is reasonably necessary for:

- (i) enforcement of the criminal law; or

---

47 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.19].

48 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 subsection 355–55(1) table item 1.

49 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

- (ii) enforcement of a law imposing a pecuniary penalty; or
- (iii) protection of the public revenue;

to an agency whose functions include that enforcement or protection, for the purposes of that enforcement or protection;

9.52 The Tax Laws Exposure Draft Bill proposes a number of changes to the provisions in taxation legislation dealing with disclosure for the purposes of law enforcement. The Bill expands the range of circumstances in which disclosures can be made to ASIC in order for it to fulfil its law enforcement role. It is proposed that disclosures will be permitted to ASIC for the enforcement of a law administered by ASIC which is a criminal law or which imposes a monetary penalty.<sup>50</sup> The Explanatory Material notes that enforcing a law includes investigating breaches of that law, prosecuting any offences committed under that law, and gathering information to support the investigation and prosecution functions.<sup>51</sup>

9.53 The Bill also proposes to amend the provisions allowing disclosure to law enforcement agencies for the enforcement of ‘serious criminal offences’.<sup>52</sup> Under the existing provisions, law enforcement agencies that receive taxpayer information for the purposes of investigating an offence cannot then use that information for the prosecution of the offence unless it is a taxation offence:

Taxpayer information has proved to be a valuable source of intelligence information for the investigation of activities such as money laundering and social security fraud. Such information would also be invaluable for and could form the basis of related prosecutions. This broadening of the disclosure also recognises the changing nature of crime and the need for flexible, whole-of-government responses. It will also ensure that law enforcement agencies can rely on the best evidence prosecution.<sup>53</sup>

9.54 The Tax Laws Exposure Draft Bill also proposes to amend the definition of ‘serious offence’ to mean an offence punishable by more than twelve months imprisonment, consistent with the Commonwealth definition of an indictable offence.<sup>54</sup>

### ***Submissions and consultations***

9.55 A number of agencies submitted that it was important to allow the exchange of information with law enforcement and regulatory agencies, and to ensure that secrecy provisions did not interfere with these processes. In its submission, the CDPP noted that:

---

50 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1, item 1, subsection 355-65(1), item 1 in table 3.

51 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.54].

52 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1, item 1, subparagraph 355-70 (1)(c)(i).

53 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.64].

54 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 s 355-70(7).

The CDPP considers that the interaction between the secrecy provisions in the legislation of investigation agencies and the criminal process can be problematic. In particular, secrecy provisions can create a very narrow basis for disclosure of information to other investigation agencies. This, in turn, impacts on the investigation of serious criminal offences ...

The CDPP is aware of matters where investigation agencies have requested information from the ATO as part of an investigation of a serious Commonwealth offence, where the ATO has been unable to provide that information, as disclosure was prevented by the taxation secrecy provisions.<sup>55</sup>

9.56 The ATO also noted that the existing taxation secrecy provisions inhibited its ability to share information with law enforcement agencies.<sup>56</sup>

9.57 The CDPP went on to note the changing nature of law enforcement and the fact that serious criminal activity is no longer confined to one identifiable area:

By way of example, those involved in trafficking narcotics will also commonly be involved in money laundering and tax evasion. Similarly, terrorist activity may not only involve acts of, or in direct preparation of, terrorism. While direct Australian experience is limited, it is generally accepted that terrorist activity may be accompanied with other forms of illegal activity, such as offences against immigration/passport laws, customs offences, money laundering, fraud, firearm offences, taxation fraud, identity fraud and social security fraud. ... Active co-operation between a range of Government agencies is important to identify, investigate and prosecute such serious criminal activity. ...

A possible reform to secrecy provisions to meet these concerns would be amendment to enable information to be disclosed where the disclosure was reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty and allowing for the use of the information as evidence in the prosecution of offences.<sup>57</sup>

9.58 The Treasury also expressed support for provisions allowing the disclosure of information to law enforcement agencies. The Treasury noted, however, that where the purpose of the disclosure is far removed from the purpose for which the information was collected, any provision allowing disclosure should be narrowly framed.<sup>58</sup>

9.59 The Department of Education, Employment and Workplace Relations noted that:

if there is a commitment to a whole of government approach to minimising fraud against the Commonwealth and protecting Australia's domestic and international interests, then there is a need to ensure that secrecy provisions do not unnecessarily constrain an agency's ability to share information with another agency that has direct responsibility for a particular regulatory function.<sup>59</sup>

---

<sup>55</sup> Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

<sup>56</sup> Australian Taxation Office, *Submission SR 13*, 16 February 2009.

<sup>57</sup> Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

<sup>58</sup> The Treasury, *Submission SR 22*, 19 February 2009.

<sup>59</sup> Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

9.60 The DHS noted that:

while Medicare Australia is able to disclose information to the police under a public interest certificate, often the police are unable to then share that information directly with prosecuting authorities and the courts. While practical workarounds are sometimes used (such as Medicare, rather than the police, making the further disclosures) the policy justification for this type of restriction could be questioned.<sup>60</sup>

#### *ALRC's views*

9.61 The ALRC recognises the importance of allowing information to flow to law enforcement and regulatory agencies in appropriate circumstances. However, the ALRC's preliminary view is that the disclosure of Commonwealth information for the purposes of law enforcement is not a matter for individual Commonwealth officers, but should be regulated at agency level, based on agency specific legislation, agency policies and guidelines and inter-agency MOUs. On this basis, such disclosures would fall within the exception for disclosure in the course of an officer's duties and functions.

9.62 If it is not clear to a particular officer whether information should be passed onto a law enforcement agency, it would also be possible, under the proposed structure of the general secrecy offence exceptions, to seek the agency head's permission and to rely on that exception.

9.63 For the purposes of this Discussion Paper, the ALRC is proceeding on the basis that the Australian Government will move forward with its proposed public interest disclosure legislation, as discussed in the House of Representatives Standing Committee on Legal and Constitutional Affairs (the Standing Committee) report, entitled *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (the *Whistleblower Protection* report).<sup>61</sup> The current proposal for public interest disclosure legislation, discussed in detail below, would provide an avenue for Commonwealth officers to report a range of matters to appropriate authorities, including serious matters related to illegal activity.

#### **For use in legal proceedings**

9.64 A number of secrecy offences expressly regulate the disclosure of Commonwealth information to the courts. As discussed in Chapter 1, the disclosure of Commonwealth information for use in legal proceedings is not a focus of this Inquiry. In relation to the general secrecy offence, however, such disclosure could be made in the course of a Commonwealth officer's functions or duties; or with the authority of the agency head or minister. Consequently, the ALRC does not propose that this be included as an express exception in the general secrecy offence.

---

60 Department of Human Services, *Submission SR 26*, 20 February 2009.

61 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

## **With consent**

9.65 As discussed in Chapter 5, some secrecy provisions provide an exception permitting the disclosure of information with the consent of the person to whom, or entity to which, the information relates.<sup>62</sup>

9.66 The Tax Laws Exposure Draft Bill does not, however, include consent as a defence for an otherwise unauthorised disclosure.<sup>63</sup> The Explanatory Material to the Draft Bill states that:

This approach avoids issues of whether the consent is informed and voluntary (as opposed to, for instance, being a precondition for a particular good or service). This also recognises the fact that, if any entity requires the taxpayer's information, the taxpayer is able to obtain that information and pass it on. Indeed, there is no prohibition on a taxation officer or a non-taxation officer in lawful receipt of taxpayer information from disclosing that information to the taxpayer and there are no limits on what a taxpayer may do with their own information. This will ensure that the taxpayer knows precisely what information is being provided.<sup>64</sup>

## ***Submissions and consultations***

9.67 The ATO suggested that there would be some administrative benefits if a taxpayer could consent to his or her information being released to a third party. For example, the ATO could provide information directly to banks to confirm taxpayers' tax details.<sup>65</sup> A number of other agencies also expressed support for allowing disclosure with consent.<sup>66</sup> APRA noted that s 56 of the APRA Act allowed the release of personal information with the consent of the individual to whom the information relates.<sup>67</sup>

9.68 In its submission, the AGD noted that:

It may be appropriate to permit disclosure of personal information with the consent of the person to whom the information relates. However, it would be important that the consent is expressly provided, voluntary and informed. The Treasury's Discussion Paper contains a useful discussion about consent, noting concerns that taxpayers could be denied a service or good if they did not consent to the Tax Office providing their confidential information to the provider of that good or service. The Paper noted an alternative approach is to enable the taxpayer to obtain their confidential information from the Tax Office and provide the necessary information to the third party.<sup>68</sup>

---

62 See, eg, *Gene Technology Act 2000* (Cth) s 187(1)(f); *National Health Act 1953* (Cth) s 135A(8); *Reserve Bank Act 1959* (Cth) s 79A(3).

63 Exposure Draft, *Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009* (Cth).

64 Explanatory Material, *Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009* (Cth), [4.15].

65 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

66 Department of Human Services, *Submission SR 26*, 20 February 2009; Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

67 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

68 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

9.69 ASIC expressed the view that a consent exception may be desirable under the ASIC Act, but noted that the exception would have to be limited so that it did not allow the disclosure of information that would harm other public interests, such as an ongoing investigation under the ASIC Act.<sup>69</sup>

#### *ALRC's views*

9.70 Disclosure of Commonwealth information with the consent of the person to whom, or entity to which, the information relates is not appropriate in all circumstances. The information may be sensitive for other reasons—for example, it may be personal information about one individual that is relevant to an ongoing investigation into the criminal activities of another individual. For this reason, the ALRC is not proposing to include disclosure with consent as an exception to the new general secrecy offence.

9.71 Where it is desirable in particular agencies to allow release of information with consent, this should be made clear in agency-specific legislation, agency policies and guidelines or inter-agency MOUs. In this way, disclosure with consent will fall within the exception provided in the general secrecy offence for disclosure in the course of a Commonwealth officer's functions and duties or disclosure with the authority of the agency head.

#### **A serious threat to a person's life, health or safety**

9.72 As discussed in Chapter 5, a number of secrecy provisions include an exception for disclosure where it is necessary to prevent or lessen a serious threat to a person's life, health or safety. For example, s 16(3F) of the *Customs Administration Act 1985* (Cth) provides that a person may disclose protected information:

if there are reasonable grounds for that person to believe that:

- (a) a serious and imminent threat to the health or life of a person or persons exists or might exist; and
- (b) it is necessary to carry out that act in order to avert or reduce that threat.

---

69 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

9.73 The Tax Laws Exposure Draft Bill proposes an exception for disclosure to a government agency where the disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety.<sup>70</sup> This exception is based on one of the exceptions in Information Privacy Principle (IPP) 11 in the *Privacy Act 1988* (Cth)—which regulates the disclosure of personal information by Australian Government agencies—for disclosure of personal information where the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of any person. The Tax Laws Exposure Draft Bill provision does not include a requirement that the threat be imminent.<sup>71</sup>

9.74 The Explanatory Material to the Draft Bill states that:

The fact that there is a threat is not enough. The disclosure of the information must be necessary to prevent or lessen the threat. A taxation officer must therefore consider whether the disclosure will have any real impact on the threat or whether there are any alternatives, other than the disclosure of taxpayer information, that could achieve the same result.

A threat to life or health includes threats to safety and would include bushfires, industrial accidents and direct threats to individuals or groups. Health includes mental as well as physical health, although a threat of stress or anxiety would generally not be sufficient.<sup>72</sup>

9.75 Some secrecy provisions allow disclosure in an even wider range of circumstances. For example, s 16 of the *Child Support (Registration and Collection) Act 1988* (Cth) allows the disclosure of protected information to any person, if the information concerns 'a credible threat to the life, health or welfare of a person' and the Registrar, or a person authorised by the Registrar, believes on reasonable grounds that the disclosure is necessary to prevent or lessen the threat.

9.76 The *Criminal Code* includes a defence of 'sudden or extraordinary emergency' where a person reasonably believes that:

- (a) circumstances of sudden or extraordinary emergency exist; and
- (b) committing the offence is the only reasonable way to deal with the emergency; and
- (c) the conduct is a reasonable response to the emergency.<sup>73</sup>

---

70 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1, s 355-90.

71 In *For Your Information: Australian Privacy Law and Practice* (ALRC 108) the ALRC recommended that the privacy principles in the *Privacy Act 1988* (Cth) should be amended to remove the requirement of 'imminence' and to allow the disclosure of personal information where necessary to lessen or prevent a serious threat to an individual's life, health or safety: Rec 25–3.

72 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.82]–[5.83].

73 *Criminal Code* (Cth) s 10.3.

9.77 The *Commonwealth Criminal Code: Guide for Practitioners* states that:

The emergency must be real or reasonably apprehended as real: The defence of sudden or extraordinary emergency is not available to a defendant who is unreasonably mistaken in apprehending a situation of emergency;

The emergency must be unavoidable by lesser means: The defence is barred unless commission of the offence was the only reasonable way to deal with the emergency;

The defendant's response to the emergency must be reasonable in the circumstances: The defence is barred if commission of an offence was not a reasonable response to the emergency.<sup>74</sup>

9.78 The *Code* defence is a general defence that would be available in relation to the proposed general secrecy offence and the subsequent disclosure offence.

#### ***Submissions and consultations***

9.79 As noted above, the AGD suggested that the general secrecy offence should include an exception for disclosures to prevent serious and imminent threats to life or health.<sup>75</sup>

9.80 The DHS noted that:

[Commonwealth Rehabilitation Service] Australia's provisions do not deal explicitly with situations where the disclosure of information might assist in a criminal investigation, or where disclosure is necessary to protect against an imminent threat to a person's life or physical safety. Currently, disclosures must be made under a public interest certificate executed by a delegate within the Department of Education, Employment and Workplace Relations. Timeliness is an issue; for example, when a person departs CRS Australia premises having threatened suicide or imminent physical harm to another, including employees at a place they are about to visit, the current secrecy provision prevents CRS Australia from taking protective action until a DEEWR delegate approves the disclosure.<sup>76</sup>

#### ***ALRC's views***

9.81 The ALRC does not propose that the general secrecy offence include an express exception for disclosures necessary to lessen or prevent a serious threat to a person's life, health or safety. The ALRC's preliminary view is that the *Criminal Code* defence of sudden or extraordinary emergency will operate to protect Commonwealth officers in appropriate circumstances. The defence would apply where a Commonwealth officer has a reasonable belief that a real threat exists—for example, as in the DHS example provided above, someone has left agency premises threatening to kill someone else—the disclosure of Commonwealth information is the only reasonable way to deal with the threat; and the disclosure is a reasonable response to the threat.

<sup>74</sup> Australian Government Attorney-General's Department and the Australian Institute of Judicial Administration, *The Commonwealth Criminal Code: A Guide for Practitioners* (2002), 227.

<sup>75</sup> Attorney-General's Department, *Submission SR 36*, 6 March 2009.

<sup>76</sup> Department of Human Services, *Submission SR 26*, 20 February 2009.

### **A serious threat to public health or public safety**

9.82 The Tax Laws Exposure Draft Bill also proposes an exception for disclosure to a government agency where the disclosure is necessary to lessen or prevent a serious threat to public health or public safety.<sup>77</sup> The Explanatory Material states that:

Threats to public health or safety are those that have the potential to affect the public (both in Australia and overseas) more generally rather than just a specific individual or group of individuals. A possible outbreak of an infectious disease is one such example, and an example of where a threat to the public health or safety would be serious.<sup>78</sup>

#### ***ALRC's views***

9.83 The ALRC does not propose that the general secrecy offence include an express exception for disclosures necessary to lessen or prevent a serious threat to public health or public safety. Where such disclosures do not fall within an officer's functions and duties, it will be open to an officer to seek agency head or ministerial authorisation for disclosure. The ALRC notes that certain such disclosures will fall within the 'sudden or extraordinary emergency' *Criminal Code* defence—that is, where the officer reasonably believed that: there was a sudden or extraordinary public health or safety emergency; the disclosure was the only reasonable way to deal with the emergency; and the disclosure was a reasonable response to the emergency.

9.84 In the *Whistleblower Protection* report,<sup>79</sup> discussed in detail below, the Standing Committee recommended that public interest disclosure legislation should protect disclosures about serious matters, including dangers to public health or public safety. This includes disclosures made to the media, where the matter threatens immediate serious harm to public health or safety and has been disclosed to internal and external authorities, but has not been acted on in a reasonable time.<sup>80</sup> A person who made such a disclosure under the public interest disclosure legislation would be protected from criminal liability, including liability under the proposed general secrecy offence.

### **Information already in the public domain**

9.85 In its submission, the AGD suggested that the ALRC consider including an exception for disclosure where the information has been made lawfully available to the public.<sup>81</sup> Regulation 2.1(5) of the *Public Service Regulations 1999* (Cth) provides an exception where information 'is already in the public domain as the result of a disclosure of information that is lawful under these Regulations or another law'. The

---

77 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1, s 355-90.

78 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.85].

79 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

80 Ibid, Rec 21.

81 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

Explanatory Memorandum to the legislative instrument that enacted the current version of reg 2.1 notes that this exception:

would not apply if at the time of disclosure the information had not yet been lawfully disclosed, for example the matter was made public via a budget ‘leak’. Nor would it apply if disclosure would have the effect of expressly or impliedly disclosing other information to which subregulations 2.1(3) and 2.1(4) apply. An example would be where a public servant makes a disclosure which, because of their official role, has the effect of confirming a previous leak of information that had been provided in confidence by another government.<sup>82</sup>

9.86 The question of information already in the public domain was considered in the *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions*:

the tax secrecy and disclosure rules protect information obtained by the Commissioner in order to maintain the public confidence. However, these rules need not protect tax information that is already in the public domain. ... While the current formulation of most secrecy and disclosure provisions allows such disclosures (according to government legal advice), this has not always been clear.<sup>83</sup>

9.87 Under the Tax Laws Exposure Draft Bill, it is not an offence to disclose information that is lawfully available to the public:

A publicly available source would include things such as the electoral roll, open court records, books, the Internet, newspapers and other material that is generally available to the public. The information does not cease to be ‘publicly available’ if a member of the public has to pay a fee to access that information.<sup>84</sup>

9.88 Section 91.2 of the *Criminal Code* provides a defence in relation to the espionage offences in s 91.1 where the relevant information is lawfully available:

- (1) It is a defence to a prosecution of an offence against subsection 91.1(1) or (2) that the information the person communicates or makes available is information that has already been communicated or made available to the public with the authority of the Commonwealth.
- (2) It is a defence to a prosecution of an offence against subsection 91.1(3) or (4) that the record of information the person makes, obtains or copies is a record of information that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matters in subsections (1) and (2). See subsection 13.3(3).

<sup>82</sup> Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006).

<sup>83</sup> The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 10–11.

<sup>84</sup> Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.30].

### ***Submissions and consultations***

9.89 The ATO considered that once information has entered the public domain, it loses its inherently confidential nature and should not be protected, regardless of its source.<sup>85</sup>

9.90 APRA noted that information that is lawfully in the public domain is excluded from the definition of ‘protected information’ in s 56 of the APRA Act.<sup>86</sup> A number of other stakeholders expressed support for including an exception along these lines.<sup>87</sup> Liberty Victoria, for example, stated that it would be arbitrary to impose criminal liability on those who disclose information that is already in the public domain:

For instance, while a journalist may be the subject of penalty for subsequent handling of secret information, a member of the public should not be punished for repeating that information once it has been published or otherwise made public.

As a result Liberty Victoria strongly supports an exception from penalty for disclosure of information already in the public domain.<sup>88</sup>

9.91 The DHS cautioned, however, that:

A difficulty in relation to a public information defence/exception centres on whether it should apply only where the disclosing employee knows, or believes on reasonable grounds, that the information is publicly known. What amounts to ‘public knowledge’ of a matter will be an issue for example where the offending material appears on the customer’s Facebook or MySpace site and not more widely.<sup>89</sup>

### ***ALRC’s views***

9.92 As discussed in Chapter 7, the proposed new general secrecy offence will impose criminal liability only where the information disclosed harms, is reasonably likely to harm, or is intended to harm specified public interests. Public interests such as national security and international relations can be harmed by the disclosure of information, even where the information is already in the public domain—for example, where information has been ‘leaked’ but there is uncertainty about whether or not the information is genuine or complete. A Commonwealth officer may harm a relevant public interest by disclosing the same information, thereby confirming that the information is genuinely Commonwealth information. The ALRC proposes, therefore, that the general secrecy offence should include an exception for disclosure of information, but only where the information is *lawfully* in the public domain.

---

85 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

86 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

87 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009; The Treasury, *Submission SR 22*, 19 February 2009; Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

88 Liberty Victoria, *Submission SR 19*, 18 February 2009.

89 Department of Human Services, *Submission SR 26*, 20 February 2009.

9.93 The issue of when information is in the public domain has been extensively considered by the courts in the context of breach of confidence. Information is in the public domain when it has received such publicity among relevant groups in the community as to effectively destroy the usefulness of its secrecy to its owner, or to destroy any usefulness in enforcing the original obligation of confidentiality.<sup>90</sup>

9.94 It is unlikely that a charge would be brought against a Commonwealth officer under the proposed new general secrecy offence for disclosure of information that is already *lawfully* in the public domain. This is because the offence requires that the disclosure harms, is reasonably likely to harm, or is intended to harm one of the specified public interests. While it is unlikely that such disclosure would harm, or be reasonably likely to harm one of the specified public interests, it is possible that a Commonwealth officer might disclose information intending to cause harm, unaware that the information is already in the public domain and so the ALRC has included the exception to ensure that the matter is absolutely clear. The exception should also be included in the proposed subsequent disclosure provision,<sup>91</sup> so that where a Commonwealth officer discloses information to a person—for example, a journalist—in breach of the general secrecy provision, and the information is later lawfully put into the public domain, the journalist will not be guilty of an offence under the subsequent disclosure provision if he or she then on-discloses the information.

**Proposal 9–1** The proposed general secrecy offence should expressly include exceptions applying where the disclosure is:

- (a) in the course of a Commonwealth officer’s functions or duties;
- (b) authorised by the relevant agency head or minister, and the agency head or minister certifies that the disclosure is in the public interest; or
- (c) of information that is already in the public domain as the result of a lawful disclosure.

## Public interest disclosure

9.95 This section of the chapter examines whether the general secrecy offence should contain an exception for disclosures that are made in the public interest. A related issue raised in the course of this Inquiry is the interaction between secrecy offences and proposed new Commonwealth public interest disclosure legislation. This section provides a brief overview of proposals in relation to whistleblower protection

<sup>90</sup> *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413.  
<sup>91</sup> Proposal 8–3.

legislation and examines how such legislation may interact with the proposed general secrecy offence.

9.96 The relationship between the proposed public interest disclosure legislation and specific secrecy offences is discussed in Chapter 11.

#### ***Public interest exceptions in secrecy provisions***

9.97 Section 70 of the *Crimes Act* does not create an exception or defence relating to the disclosure of information ‘in the public interest’. While s 79 of the *Crimes Act* permits a person to communicate prescribed information to a ‘person to whom it is, in the interests of the Commonwealth ... his or her duty to communicate it’,<sup>92</sup> the meaning and scope of this exception is unclear.<sup>93</sup>

9.98 As noted in Chapter 5, some secrecy provisions in Commonwealth legislation include more confined exceptions that permit certain disclosures in the public interest. However, such disclosures are generally only permitted by senior officers and for limited purposes. For example, the *Law Enforcement Integrity Commissioner Act 2006* (Cth) permits the Integrity Commissioner to disclose certain information ‘if [he or she] is satisfied that it is in the public interest to do so’.<sup>94</sup> Similarly, the *Australian Security Intelligence Organisation Act 1979* (Cth) (the ASIO Act) allows the disclosure of information where the information concerns matters outside Australia and the Director-General of ASIO ‘is satisfied that the national interest requires the communication’.<sup>95</sup>

9.99 Occasionally, legislation provides that a minister may determine that a disclosure is in the public interest. For example, the *Food Standards Australia New Zealand Act 1991* (Cth) permits the disclosure of certain information if the responsible minister certifies, by instrument, that it is necessary ‘in the public interest’.<sup>96</sup>

#### ***Public interest disclosure legislation***

9.100 Public interest disclosure, or ‘whistleblowing’, is ‘the disclosure by organisation members (former or current) of illegal, immoral or illegitimate practices under the control of their employers to people or organisations that might be able to effect action’.<sup>97</sup> Public interest disclosures by Commonwealth officers may involve the disclosure of information obtained because of a person’s position as a Commonwealth officer, and therefore may attract criminal penalties under various secrecy offences.

9.101 Currently, there is limited protection at the Commonwealth level for people who make public interest disclosures. As discussed in Chapter 15, s 16 of the *Public Service*

92 *Crimes Act 1914* (Cth) ss 79(2)(a)(ii), 79(3)(b).

93 This exception is discussed further in Ch 5.

94 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 209.

95 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(b).

96 *Food Standards Australia New Zealand Act 1991* (Cth) s 114(4). See also *Medical Indemnity Act 2002* (Cth) s 77(3); *Health Insurance Act 1973* (Cth) s 130(3); *National Health Act 1953* (Cth) s 135A(3).

97 A Brown, *Public Interest Disclosure Legislation in Australia* (2006), xxi.

*Act 1999* (Cth), entitled ‘Protection for whistleblowers’, provides that a person performing functions for an Australian Government agency must not victimise or discriminate against an Australian Public Service (APS) employee who has reported breaches of the APS Code of Conduct to the Public Service Commissioner, Merit Protection Commissioner or the head of an agency. This provision is quite limited in scope. Importantly, it does not provide protection against criminal liability under secrecy laws. Professor AJ Brown has suggested that, at the Commonwealth level, there is no protection from

the legal or disciplinary consequences that might attach to an APS employee who reports a breach of the APS Code of Conduct. At best s 16 of the [Public Service Act] can be taken as relieving a whistleblower from liability to disciplinary action if the action could be shown to constitute victimisation or discrimination for the reporting of a breach.<sup>98</sup>

9.102 Some Commonwealth legislation contains more comprehensive protection for whistleblowers working in particular areas. For example, the *Aged Care Act* provides immunity from prosecution for a person who makes a disclosure (in accordance with the reporting framework in the Act) regarding the assault of a person in residential care.<sup>99</sup> Both the *Workplace Relations Act 1996* (Cth) and the *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) provide certain persons with protection in relation to disclosure of information that reasonably indicates that there has been a contravention of the legislation. The protection provided includes immunity against ‘any civil or criminal liability for making the disclosure’.<sup>100</sup>

9.103 All Australian states and territories have enacted legislation to facilitate the making of public interest disclosures and to protect people who make them.<sup>101</sup> This legislation is intended, among other things, to provide immunity from prosecution for offences associated with breaches of state or territory secrecy provisions. For example, the *Whistleblowers Protection Act 2001* (Vic) provides that a person who makes a ‘protected disclosure’ does not ‘commit an offence under ... a provision of any other Act that imposes a duty to maintain confidentiality with respect to a matter or any other restriction on the disclosure of information’.<sup>102</sup>

### **Whistleblower Protection report**

9.104 As noted above, the House of Representatives Standing Committee on Legal and Constitutional Affairs (the Standing Committee) issued the *Whistleblower*

---

98 Ibid, 34.

99 *Aged Care Act 1997* (Cth) s 96-8.

100 *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) pt 10-5; *Workplace Relations Act 1996* (Cth) sch 1, pt 4A.

101 *Protected Disclosures Act 1994* (NSW); *Whistleblowers Protection Act 2001* (Vic); *Whistleblowers Protection Act 1994* (Qld); *Public Interest Disclosure Act 2003* (WA); *Whistleblowers Protection Act 1993* (SA); *Public Interest Disclosures Act 2002* (Tas); *Public Interest Disclosure Act 1994* (ACT); *Public Interest Disclosure Act 2008* (NT).

102 *Whistleblowers Protection Act 2001* (Vic) s 15.

*Protection* report in February 2009.<sup>103</sup> The Standing Committee recommended that the Australian Government introduce public interest disclosure legislation to provide whistleblower protections in the Australian Government public sector.<sup>104</sup> The proposed legislation would establish a system whereby employees in the Commonwealth public sector can make disclosures about serious matters within their organisation, to other public service agencies or, in limited circumstances, publicly.

9.105 The Standing Committee recommended that the proposed legislation cover a broad range of participants in the Australian Government public sector, including:

- Australian Government and general government sector employees including APS employees;
- contractors and consultants engaged by the public sector and their employees;
- Australian and locally engaged staff working overseas;
- members of the Australian Defence Force and Australian Federal Police (AFP);
- parliamentary staff;
- former employees in any of the above categories; and
- anonymous persons likely to be in any of the above categories.<sup>105</sup>

9.106 The types of disclosure protected by the proposed public interest disclosure legislation would include, but not be limited to, ‘serious matters’ related to illegal activity, corruption, maladministration, breach of public trust, scientific misconduct, wastage of public funds, dangers to public health or safety, dangers to the environment, official misconduct (including breaches of codes of conduct) and adverse action against a person who makes a public interest disclosure.<sup>106</sup> A person making a disclosure must have an honest and reasonable belief, on the basis of information available to them, that the matter concerns disclosable conduct under the legislation.<sup>107</sup>

9.107 The Standing Committee also made recommendations regarding procedures to facilitate the making of a public interest disclosure, and proposed that a person could make a public interest disclosure internally (that is, to the agency concerned) or

---

103 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

104 Ibid, Rec 1.

105 Ibid, Rec 3.

106 Ibid, Rec 7.

107 Ibid, Rec 10.

externally (to the Commonwealth Ombudsman, Australian Public Service Commissioner or other integrity agency) or both.<sup>108</sup>

9.108 A person who made a disclosure under the framework established by the proposed legislation would be protected from detrimental action in the workplace and receive immunity from criminal liability (including under secrecy offences),<sup>109</sup> civil liability (including civil penalties and civil actions) and administrative sanctions.

9.109 The Standing Committee considered that it was necessary to protect public interest disclosures to third parties—such as to the media, a member of parliament, a trade union or a legal adviser—in certain circumstances. The Standing Committee stated that:

experience has shown that internal processes can sometimes fail and people will seek alternative avenues to make their disclosure.

There are cases with implications of the utmost seriousness, when disclosure through third parties has been initially necessary and consequently beneficial. ... A public interest disclosure scheme that does not provide a means for such matters to be brought to light will lack credibility.<sup>110</sup>

9.110 Further, the Standing Committee considered that:

It may be possible that in some cases, for example, where an agency has not fulfilled its obligations to a whistleblower, the disclosure framework within the public sector may not adequately handle an issue and that a subsequent disclosure to the media could serve the public interest.<sup>111</sup>

9.111 However, the Standing Committee's final recommendation confined protected public interest disclosures to third parties to very narrow circumstances. A disclosure to a third party external to the public service would only be protected where the matter already had been disclosed internally or to an external authority, but had not been acted on in a reasonable time—having regard to the nature of the matter—and the matter threatened immediate serious harm to public health and safety.<sup>112</sup>

9.112 This recommendation with respect to disclosures to third parties has been criticised as too limited. Brown has commented that, while it is reasonable to require people to proceed through internal channels or external integrity agencies before disclosing a matter publicly, the requirement that the matter must 'threaten immediate serious harm to public health and safety' is too restrictive in that it excludes from protection public interest disclosures to the media regarding major fraud, corruption and major abuses of power. Brown also argues that the recommended provision fails to cover the situation in which the external agency does not adequately address a public

---

108 Ibid, Recs 15–19.

109 Ibid, Rec 14.

110 Ibid, [8.72]–[8.73].

111 Ibid, [8.77].

112 Ibid, Rec 21.

interest disclosure, so that ‘even if the Ombudsman had looked at the problem and failed to act, or got it wrong, a public servant who justifiably went public could still be sacked, sued or prosecuted’.<sup>113</sup>

### **Submissions and consultations**

9.113 In IP 34, the ALRC asked what relationship should exist between exceptions and defences provided under Commonwealth secrecy laws and possible new Commonwealth public interest disclosure legislation. In particular, the ALRC sought stakeholders’ views on whether public interest disclosure should be incorporated as an exception to secrecy offences.<sup>114</sup>

9.114 Several stakeholders suggested that secrecy offences should provide for an exception or defence where a disclosure could be shown to be in the public interest.<sup>115</sup> For example, the Australian Press Council expressed the view that:

First, it is essential that any legislative provision establishing an offence for unauthorised disclosure exempts from its scope those disclosures made for public interest reasons. Such reasons should include, but not be restricted to, the exposing of maladministration. If public interest disclosures are not exempt from the scope of the offence, the legislation should include a defence for the making of disclosures which are in the public interest or which are made for public interest purposes.<sup>116</sup>

9.115 The Press Council also submitted that:

With specific regard to public interest disclosures, it is not appropriate to impose a custodial sentence where the disclosure was made for the purpose of exposing maladministration. Nor should a custodial sentence be imposed unless the offender had a clear intention of obtaining benefit or had a malicious intent. The onus for establishing such intent should be on the prosecution.<sup>117</sup>

9.116 A number of comments about the need to protect ‘whistleblowers’ from prosecution under secrecy laws were made in the course of the national secrecy phone-in.<sup>118</sup> Several submissions also expressed strong support for the introduction of robust public interest disclosure legislation, noting that disclosures made under such a regime should not attract civil, criminal or administrative penalties.<sup>119</sup>

---

113 Ibid.

114 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 4–6.

115 Whistleblowers Australia, *Submission SR 40*, 10 March 2009; NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009; Community and Public Sector Union, *Submission SR 32*, 2 March 2009; Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009.

116 Australian Press Council, *Submission SR 16*, 18 February 2009.

117 Ibid.

118 *Secrecy Phone-In*, 11–12 February 2009.

119 Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009; Australian Press Council, *Submission SR 16*, 18 February 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009.

9.117 Brown submitted that the approach to disclosure to third parties proposed in the *Whistleblower Protection* report was too narrow and

fails to contemplate what would occur in circumstances where an official had reason to believe not only that their own agency would not respond appropriately to the disclosure, but that the ability of the relevant external integrity agency to respond appropriately had also been corrupted or compromised.<sup>120</sup>

9.118 Brown suggested that a better approach would be one that protects public interest disclosures to persons outside government:

- where the matter has been disclosed internally to the agency concerned and to an external integrity agency of government, or to an external integrity agency alone, and has not been acted on in a reasonable time having regard to the nature of the matter; or
- where a matter is exceptionally serious, and special circumstances exist such as to make the prior disclosure of the matter, internally or to an external integrity agency, either impossible or unreasonable (for example, in some circumstances involving a serious and immediate threat to public health or safety).<sup>121</sup>

9.119 In Professor Brown's view, if this issue is not adequately addressed in public interest disclosure legislation, it will be necessary to include an appropriate exception or defence in relevant secrecy offences. On the other hand, ASIC highlighted the need for caution in linking public interest disclosure legislation with secrecy provisions, noting that a public interest disclosure may have the potential to harm the public interest and that, in the public interest disclosure context, a decision would have to be made about the relative merits of the competing public interests.<sup>122</sup>

### ALRC's views

9.120 At the time of writing, the Australian Government had not responded to the *Whistleblower Protection* report. While the Government has indicated that it intends to develop public interest disclosure legislation in 2009,<sup>123</sup> the ALRC may not have the opportunity to consider the final form of the legislation before this Inquiry's final Report is due. For the purposes of this Discussion Paper, the ALRC is proceeding on the basis that any future public interest disclosure legislation will largely reflect the recommendations made in the *Whistleblower Protection* report. The ALRC recognises, however, that the final form of the legislation may differ from those recommendations.

9.121 Because the whistleblower protections recommended by the Standing Committee include immunity from criminal liability, it may not be necessary to include an express exception in the general secrecy offence for disclosures made in the public

---

120 AJ Brown, *Submission SR 44*, 18 May 2009.

121 Ibid.

122 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

123 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <<http://www.smos.gov.au/speeches>> at 6 May 2009.

interest. A public interest disclosure exception would provide no additional protection for a person immune from criminal liability under public interest disclosure legislation. For the sake of clarity, it would be useful to include a legislative note in the general secrecy offence referring to the fact that public interest disclosure legislation may provide immunity from criminal liability for a breach of the secrecy offence.

9.122 For this interaction to be effective, however, there needs to be consistency between the proposed general secrecy offence and the proposed public interest disclosure legislation. In particular, it is important that the public interest disclosure legislation cover at least the same categories of persons covered by the general secrecy offence. There also needs to be adequate protection for individuals who make public interest disclosures to third parties, such as the media, and those who may be caught by the ALRC's subsequent disclosure offence.

#### *Categories of persons covered*

9.123 To provide effective protection for whistleblowers, the public interest disclosure legislation should cover at least the same range of persons as those subject to the general secrecy offence. If the legislation fails to cover some persons subject to the general secrecy offence, such people who disclose information in the public interest would not receive immunity from prosecution for contravention of the secrecy offence.

9.124 The ALRC proposes that the new general secrecy offence cover a range of 'Commonwealth officers'.<sup>124</sup> Of these people, it appears that only the Governor-General, ministers and parliamentary secretaries would not be covered by the proposed public interest disclosure legislation. While the *Whistleblower Protection* report did not expressly consider the issue, it may be that people so senior in the executive branch of government have alternative avenues to make public interest disclosures and do not require whistleblower protection—for example, members of parliament are protected from criminal and other liability for disclosures made under the protection of parliamentary privilege.<sup>125</sup> Otherwise, the categories of people subject to the proposed secrecy offence and those the Standing Committee proposes be covered by the public interest disclosure legislation seem consistent, albeit expressed in different language. The statutory language used in the public interest disclosure legislation and the proposed new general secrecy offence ultimately should be consistent in this regard.

9.125 The *Whistleblower Protection* report recommended that public interest disclosure legislation provide that a decision-maker within the scheme be able to deem a person to be a public official for the purposes of the legislation, where that person has an 'insider's knowledge' of matters that might form the basis of a public interest

---

124 See Proposal 7–2.

125 Parliamentary privilege is discussed in Ch 2.

disclosure.<sup>126</sup> The Standing Committee used the example of a former volunteer of a not-for-profit body contracted to a local government authority to implement a federally funded program. The Standing Committee expressed the view that ‘there should be no automatic protection afforded to people in such instances but a decision maker should be able to grant protection in appropriate circumstances’.<sup>127</sup> It could be that one consideration in making a decision to deem a person to be a ‘public official’ for the purposes of public interest disclosure legislation might be whether he or she is subject to a secrecy offence.

#### ***Public interest disclosures to third parties***

9.126 A person making a disclosure to a third party in the public interest that relates to a serious matter, but which does not threaten immediate serious harm to public health and safety, would not receive immunity from liability under the public interest disclosure legislation proposed by the Standing Committee. Concerns have been expressed that the provision recommended by the Standing Committee is too narrow.<sup>128</sup> Arguably, a person who publicly discloses information relating to a particularly serious matter in the public interest, where other avenues of disclosure are exhausted or unavailable, should not be liable to prosecution for contravention of a secrecy offence.

9.127 It is also important to ensure that a journalist or other person who further discloses information received by way of a public interest disclosure will not commit an offence—for example, under offences which cover the disclosure of information by ‘any person’<sup>129</sup> or under the proposed subsequent disclosure offence.<sup>130</sup> While this issue does not appear to have been directly considered by the Standing Committee, it seems logical that a third party who subsequently discloses information received by way of a protected public interest disclosure would also be immune from civil or criminal liability.

#### ***Conclusion***

9.128 The ALRC considers that comprehensive public interest disclosure legislation is preferable to developing a public interest exception to the general secrecy offence. An exception to the secrecy offence would only provide a person making a public interest disclosure with protection against criminal prosecution, whereas a comprehensive

---

126 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 5.

127 Ibid, [3.85].

128 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Inquiry into Whistleblowing Protections Within the Australian Government Public Sector: Terms of Reference* (2008) Parliament of Australia, [8.35]–[8.48].

129 For example, *Crimes Act 1914* (Cth) s 79.

130 Proposal 8–3.

public interest disclosure scheme would also give whistleblowers immunity from civil and administrative sanctions.

9.129 However, if the public interest disclosure legislation provides insufficient protection for public interest disclosures to third parties, or the proposed legislation is not enacted, it would become necessary to consider an exception to any new general secrecy offence and the subsequent disclosure offence for such public interest disclosures. The exception could encompass a broader range of public interest disclosures than recommended in the *Whistleblower Protection* report. For example, an alternative based on Brown's approach, discussed above, would be to protect disclosures made where:

- the matter has been disclosed to the proper authorities and has not been acted on in a reasonable time having regard to the nature of the matter; or
- the matter is exceptionally serious, and special circumstances exist such as to make the prior disclosure of the matter to the proper authorities either impossible or unreasonable (for example, a serious and immediate threat to public health or safety).<sup>131</sup>

9.130 The ALRC would welcome stakeholders' views on when, and in what circumstances, it would be appropriate for a public interest disclosure made to a third party to be an exception to the general secrecy offence.

**Proposal 9–2** The proposed general secrecy offence should include a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.

## Penalties

9.131 The Terms of Reference for this Inquiry ask the ALRC to consider options for ensuring a consistent approach across government to the protection of Commonwealth information. The *Guide to Framing Commonwealth Offences* directs those framing offences to 'ensure [the] penalty fits with other penalties in Commonwealth law'.<sup>132</sup> In *Same Crime, Same Time: Sentencing of Federal Offenders* (ALRC 103), the ALRC emphasised the importance of imposing consistent sentences on offenders for similar offences.<sup>133</sup> This can only be achieved if the penalties specified for similar offences are

131 AJ Brown, *Submission SR 44*, 18 May 2009.

132 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 38.

133 Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), Rec 5–1(d).

also consistent. In the following section of the chapter, the ALRC, in keeping with this approach, proposes a three tier penalty regime for the proposed general secrecy offence, and considers what penalty should apply for breach of the proposed subsequent disclosure offence.

### **Penalties in existing secrecy provisions**

9.132 Currently, both ss 70 and 79(3) of the *Crimes Act* stipulate a maximum penalty of imprisonment for two years. Section 4B of the *Crimes Act* provides a formula for the calculation of a maximum fine where a provision specifies a maximum term of imprisonment but is silent on the maximum fine. Under this provision, where a natural person is convicted of an offence against ss 70 or 79(3), if the court thinks it appropriate in all the circumstances of the case, the court may impose instead of, or in addition to, a penalty of imprisonment, a pecuniary penalty not exceeding 120 penalty units.<sup>134</sup>

9.133 Section 4B(3) provides that where a body corporate is convicted of an offence, the court may, if the contrary intention does not appear and the court thinks fit, impose a pecuniary penalty not exceeding an amount equal to five times the amount of the maximum pecuniary penalty that could be imposed by the court on a natural person convicted of the same offence.

9.134 Sections 70 and 79(3) do not require the prosecution to establish that the unauthorised disclosure caused harm, was reasonably likely to cause harm or was intended to cause harm to any specified public interest. Where an element of this nature is present in similar existing offences, the maximum penalties prescribed tend to be higher. For example, s 79(2) sets out an offence for communicating certain prescribed information ‘with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen’s dominions’. This offence stipulates a maximum penalty of seven years.

9.135 Section 142.2 of the *Criminal Code* includes an offence for using official information where a Commonwealth public official intended to dishonestly obtain a benefit for himself or herself or for another person; or dishonestly cause a detriment to another person. This offence stipulates a maximum penalty of five years.

9.136 Section 22(1) of the *Witness Protection Act 1994* (Cth) prohibits the disclosure of information about the identity or location of a person who is or has been a participant in the National Witness Protection Program, where the disclosure compromises the person’s security. This offence also attracts a maximum penalty of 10 years imprisonment.

---

134 Currently, this amounts to \$13,200: *Crimes Act 1914* (Cth) s 4AA.

9.137 The *Criminal Code* espionage offences—which include communicating information concerning the Commonwealth’s security or defence to another country intending to prejudice the Commonwealth’s security or defence—attract a maximum penalty of 25 years.

9.138 The *Surveillance Devices Act 2004* (Cth) provides an example of a secrecy offence provision with two clear tiers. The first tier does not require proof of harm, the second tier does require proof of harm. Section 45(1) prohibits the unauthorised use, recording or disclosure of protected information and prescribes a maximum penalty of two years imprisonment. Section 45(2) prohibits the same conduct where it ‘endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence’. This section provides a maximum penalty of 10 years imprisonment.

9.139 In sentencing a federal offender, s 16A(2) of the *Crimes Act* requires a court to take into account certain factors, including the ‘nature and circumstances of the offence’ and ‘any injury, loss or damage resulting from the offence’. The ‘nature and circumstances’ of the offence might include, for example, the sensitivity of the information disclosed. The ‘injury, loss or damage resulting from the offence’ would include the consequences of disclosure, for example, whether and to what degree the disclosure harmed national security or posed a risk to an individual’s life or safety.

### **Submissions and consultations**

9.140 There was some support from stakeholders for a tiered penalty structure for the proposed new general secrecy offence, with escalating penalties attaching to increasingly serious behaviour. The AGD noted in its submission that currently most secrecy offences carry a maximum penalty of two years but that, where particularly sensitive or national security information was involved, this would justify the imposition of higher maximum penalties:

The underlying principle for the imposition of higher maximum penalties in this latter category of offences is that there are certain types of Commonwealth information, the unauthorised disclosure of which could cause significant harm to the public interest and as such require additional protection. By its nature, the unauthorised disclosure of national security information will carry a higher likelihood of harm to the public interest. For example, national security information that has been received from sensitive sources such as foreign governments could not only damage international relations with that government but also jeopardise the security or defence of Australia.<sup>135</sup>

9.141 In its submission, ACLEI noted that s 127A of the *Police Regulation Act 1958* (Vic) includes two tiers. The first tier addresses the unauthorised disclosure of official information and imposes a maximum penalty of two years imprisonment, or 240 penalty units, or both. The second tier addresses the unauthorised disclosure of official

---

135 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

information where the officer knows, or is reckless as to whether, the information may be used to harm specified public interests including endangering the life or safety of any person, or impeding or interfering with the administration of justice. This offence attracts a maximum penalty of five years imprisonment, or 600 penalty units, or both.

9.142 ACLEI was of the view that, where there is an element of corrupt intent, secrecy offences ought to carry a penalty of no less than seven years. ACLEI also suggested that it might be appropriate to apply strict liability in relation to certain harmful results—for example, a disclosure that might ‘seriously prejudice the effectiveness of an authorised law enforcement operation’—but that the penalties for such an offence should be reduced.<sup>136</sup>

9.143 Liberty Victoria suggested a sliding scale of criminal penalties:

If there was intent to mishandle the information, a criminal penalty should be applied. Liberty Victoria submits that this should be on a sliding scale of punishment applied by the courts based on a number of factors including the classification of the information, and whether or not the conduct was intended to cause harm to the ‘national interest’.<sup>137</sup>

9.144 The AFP stated that:

The AFP is supportive of the idea of an offence hierarchy with a basic offence provision supported by more serious offence provisions with higher penalties that could apply in aggravated circumstances. For example, greater penalty provisions should apply in cases of a deliberate disclosure to cause damage to the government/public interest or to obtain a financial gain.<sup>138</sup>

9.145 The Australian Press Council submitted that:

The key point is that the penalty should be appropriate to the offence, taking into account both the seriousness of the breach, the purpose for which the information was disclosed and its consequences. It is not appropriate to impose a significant penalty where the information disclosed is merely trivial, where there has been no significant damage to the public interest (or no risk of such damage), where the offender has been negligent rather than reckless, or where there was an absence of intent.<sup>139</sup>

### ALRC’s views

9.146 In Chapter 7, the ALRC proposes a three tier general secrecy offence as follows:

- (1) *First tier*: a Commonwealth officer discloses Commonwealth information and the disclosure harms, or is reasonably likely to harm, one of the specified public interests. Strict liability attaches to the physical element of harm to

---

136 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

137 Liberty Victoria, *Submission SR 19*, 18 February 2009.

138 Australian Federal Police, *Submission SR 33*, 3 March 2009.

139 Australian Press Council, *Submission SR 16*, 18 February 2009.

one of the specified public interests. The prosecution is not required to prove a fault element in relation to the harm.

- (2) *Second tier:* a Commonwealth officer discloses Commonwealth information and knows, is reckless as to whether, or intends the disclosure will:
  - (i) have a substantial adverse effect on personal privacy; or
  - (ii) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation.
- (3) *Third tier:* a Commonwealth officer discloses Commonwealth information and knows, is reckless as to whether, or intends the disclosure will:
  - (i) harm the national security, defence or international relations of the Commonwealth;
  - (ii) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
  - (iii) endanger the life or physical safety of any person; or
  - (iv) pose a serious threat to public health or public safety.<sup>140</sup>

#### *First tier*

9.147 In relation to the first tier offence, the ALRC proposes that the penalty should be a maximum of two years imprisonment, or a pecuniary penalty not exceeding 120 penalty units, or both. This is consistent with most existing secrecy provisions and the fact that the proposed offence does not involve reckless or intentional harm to the public interest.

#### *Second tier*

9.148 In relation to the second tier offence, the ALRC proposes a maximum penalty of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both. The harms set out in the second tier offence do not involve risks to individual lives or community safety, unlike the harms reflected in the third tier offence. They are essentially harms to private interests. The mid-range penalty is intended to reflect the reckless or intentional nature of the harm caused and the fact that the disclosure must have a substantial adverse effect. This is consistent with the AGD *Guide to Framing*

---

140 Proposal 7–2.

*Commonwealth Offences*, which sets a penalty benchmark of five years imprisonment or 300 penalty units for offences such as corruption and abuse of public office.<sup>141</sup>

### **Third tier**

9.149 In relation to the third tier offence, the ALRC proposes a maximum penalty of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both. This offence involves harm of a high order and may involve risks to individual lives or the safety of the Australian community. A maximum penalty of seven years imprisonment is consistent with the AGD *Guide to Framing Commonwealth Offences* which states that ‘a heavier penalty will be appropriate where … the consequences of the commission of the offence are particularly dangerous or damaging’.<sup>142</sup>

9.150 This is also consistent with the position the ALRC adopted in *Fighting Words: A Review of Sedition Laws in Australia* (ALRC 104) in relation to s 80.2 of the *Criminal Code* each carry a maximum penalty of seven years imprisonment. Although the ALRC recommended that a number of the offences be repealed, after consideration the ALRC did not recommend any changes to the seven year maximum penalties imposed for the remaining offences of urging the overthrow of the government,<sup>144</sup> urging interference with parliamentary elections<sup>145</sup> and urging violence within the community.<sup>146</sup>

**Proposal 9–3** The general secrecy offence should have three tiers and three penalty levels:

- (a) Where strict liability attaches to the requirement to prove harm, the penalty should be a maximum of two years imprisonment, or a pecuniary penalty not exceeding 120 penalty units, or both.
- (b) Where a Commonwealth officer knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:
  - (i) have a substantial adverse effect on personal privacy; or
  - (ii) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation,

<sup>141</sup> Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 43.

<sup>142</sup> Ibid, 35.

<sup>143</sup> Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), [12.86]–[12.88].

<sup>144</sup> *Criminal Code* (Cth) s 80.2(1).

<sup>145</sup> Ibid s 80.2(3).

<sup>146</sup> Ibid s 80.2(5).

the penalty should be a maximum of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both.

- (c) Where a Commonwealth officer knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:
  - (i) harm the national security, defence or international relations of the Commonwealth;
  - (ii) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
  - (iii) endanger the life or physical safety of any person; or
  - (iv) pose a serious threat to public health or public safety

the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.

### **Penalties for subsequent disclosure**

9.151 In Chapter 8, the ALRC proposes the creation of an offence for the subsequent disclosure of Commonwealth information in certain circumstances. The offence would be committed where a person knew, or was reckless as to whether, information had been disclosed by a Commonwealth officer in breach of the general secrecy offence. It would also be necessary to show that the person knew, or was reckless as to whether, the subsequent disclosure of the information would harm, or was reasonably likely to harm, one of the specified public interests.<sup>147</sup>

9.152 In IP 34, the ALRC asked whether the maximum penalties for initial and subsequent disclosures should be consistent.<sup>148</sup> Examples of provisions which impose the same penalty for initial and subsequent disclosures of protected information can be found in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)<sup>149</sup> and the *Aged Care Act 1997* (Cth).<sup>150</sup>

---

147 Proposal 8–3.

148 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–5.

149 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 121(2), 127.

150 *Aged Care Act 1997* (Cth) ss 86–2, 86–5.

9.153 The *Guide to Framing Commonwealth Offences* sets out penalty benchmarks for certain classes of offences.<sup>151</sup> It specifies a penalty benchmark for breach of a confidentiality requirement as two years imprisonment or 120 penalty units—citing as examples provisions which relate to both initial<sup>152</sup> and subsequent<sup>153</sup> unauthorised handling of Commonwealth information.

### **Submissions and consultations**

9.154 In its submission, the AGD expressed the view that:

If the fault elements and harm caused by the conduct are the same, it would be reasonable for the penalty to be the same regardless of whether the offence is one of first or subsequent unauthorised handling. The penalties that apply to existing comparable offences should be considered in setting penalties. For example if an individual is aware that the disclosure of certain protected information will prejudice Australia's security it would be appropriate to apply the same penalty regardless of whether it was an initial or subsequent unauthorised disclosure.<sup>154</sup>

9.155 A number of other stakeholders agreed that the same penalty should apply to both initial and subsequent disclosures, with ASIC noting that the potential harm arising from both the initial and subsequent disclosures is the same.<sup>155</sup>

9.156 On the other hand, PIAC's view was that the penalties for subsequent disclosure should be lower, ‘except where intent to damage Australia’s national interest is proven’.<sup>156</sup>

9.157 The Australian Press Council noted that journalists and editors are not subject to the same legislative and administrative duties as Commonwealth officers and expressed concern that ‘a minor disclosure that is ostensibly in the public interest is treated as a breach of secrecy warranting criminal conviction’.<sup>157</sup>

### **ALRC’s views**

9.158 The first tier general secrecy offence imposes liability where a Commonwealth officer discloses information that harms, or is reasonably likely to harm, one of the specified public interests. The subsequent disclosure provision does not include a parallel strict liability offence. The ALRC does not consider it appropriate to impose criminal liability on non-Commonwealth officers for disclosure of Commonwealth

<sup>151</sup> Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 47.

<sup>152</sup> *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).

<sup>153</sup> *Australian Hearing Services Act 1991* (Cth) s 67(8).

<sup>154</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

<sup>155</sup> Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009. See also The Treasury, *Submission SR 22*, 19 February 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

<sup>156</sup> Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

<sup>157</sup> Australian Press Council, *Submission SR 16*, 18 February 2009.

information unless the person is reckless, knows or intends that the disclosure would cause harm.

9.159 As noted above, the proposed subsequent disclosure offence requires that the person making the subsequent disclosure:

- knew, or was reckless as to whether the information was disclosed in breach of the general secrecy offence; and
- knew, was reckless as to whether, or intended that the disclosure would harm one of the specified public interests.

9.160 The level of culpability contained in the proposed subsequent disclosure offence provision is of a similar order to that reflected in the second and third tiers of the general secrecy offence.

9.161 The ALRC proposes, therefore that a two tier penalty regime should apply to the subsequent disclosure offence. The penalties imposed should be the same as the penalties imposed in relation to the second and third tiers of the general secrecy offence.

**Proposal 9–4** Where a person knows that, or was reckless as to whether, Commonwealth information has been disclosed in breach of the general secrecy offence, and then discloses that information knowing, or reckless as to whether, or intending that the subsequent disclosure of Commonwealth information will:

- (a) have a substantial adverse effect on personal privacy; or
- (b) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation,

the penalty should be a maximum of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both.

**Proposal 9–5** Where a person knows that, or was reckless as to whether, Commonwealth information has been disclosed in breach of the general secrecy offence, and then discloses that information knowing, or reckless as to whether, or intending that the subsequent disclosure of Commonwealth information will:

- (a) harm the national security, defence or international relations of the Commonwealth;

- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
- (c) endanger the life or physical safety of any person; or
- (d) pose a serious threat to public health or public safety,

the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.

## Other issues

### Consent of the Attorney-General

9.162 The consent of the Attorney-General must be obtained before a prosecution can be commenced for breach of certain secrecy provisions. For example, the Attorney-General, or a person acting under his or her direction, must consent prior to a prosecution under s 79 or of the *Crimes Act*<sup>158</sup> or s 91.1 of the *Criminal Code* dealing with espionage. The Revised Explanatory Memorandum for the Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth) justified the need for such consent on the basis that prosecutions under Part 5.2 of the *Criminal Code*—which includes s 91.1—are likely to raise issues regarding matters of national security or sensitive international relations that require government to government contact.<sup>159</sup>

9.163 Other secrecy provisions that require the consent of the Attorney-General include:

- ss 18 and 92 of the *Australian Security Intelligence Organisation Act*, which govern communication of intelligence by officers of ASIO, and publication by any person of the identity of an officer of ASIO, respectively; and
- various provisions of the *Intelligence Services Act 2001* (Cth), including the communication of information prepared by or on behalf of ASIS, the Defence Imagery and Geospatial Organisation (DIGO) or the Defence Signals

<sup>158</sup> *Crimes Act 1914* (Cth) s 85. The Attorney-General's consent is not required for prosecutions under s 70 of the *Crimes Act*.

<sup>159</sup> Revised Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth).

Directorate (DSD) by officers of the respective agency,<sup>160</sup> and publication by any person of the identity of the staff of these agencies.<sup>161</sup>

9.164 Other types of offences that require the Attorney-General's consent in order to commence prosecutions include:

- sedition;<sup>162</sup>
- those involving harming Australians outside of Australian territory;<sup>163</sup> and
- genocide, crimes against humanity, war crimes and crimes against the administration of justice in the International Criminal Court.<sup>164</sup>

9.165 The primary justification for a requirement for the Attorney-General (or another minister or office holder) to consent to a prosecution is that it provides an additional safeguard to ensure that prosecutions are not brought in inappropriate circumstances.<sup>165</sup> The CDPP's *Prosecution Policy of the Commonwealth* advises that a consent provision may be included, for example, where 'it was not possible to define the offence so precisely that it covered the mischief aimed at and no more' or for offences that 'involve a use of the criminal law in sensitive or controversial areas, or must take account of important considerations of public policy'.<sup>166</sup>

9.166 In 1996, with respect to the repeal of certain provisions requiring the Attorney-General's consent to prosecution, the then Attorney-General, the Hon Daryl Williams AM QC MP, observed that consent provisions were originally enacted for the purpose of deterring private prosecutions brought in inappropriate circumstances—particularly for offences relating to national security or international treaty obligations:

However, since establishing the office of the Commonwealth Director of Public Prosecutions the retention of those provisions is difficult to justify. That is particularly so now that the Director of Public Prosecutions has the power to take over and discontinue a private prosecution brought in relation to a Commonwealth offence.<sup>167</sup>

---

160 *Intelligence Services Act 2001* (Cth) ss 39, 39A and 40, respectively.

161 Ibid s 41. See also *Intelligence Services Act 2001* (Cth) sch 1, pt 2, which requires the consent of the Attorney-General to prosecute members of the Committee on Intelligence and Security.

162 *Criminal Code* (Cth) s 80.5.

163 Ibid s 115.6.

164 Ibid s 268.121.

165 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <www.cdpp.gov.au/Publications/ProsecutionPolicy/> at 26 August 2008, [2.25].

166 Ibid, [2.27].

167 Commonwealth, *Parliamentary Debates*, House of Representatives, 4 December 1996, 7714, (D Williams—Attorney-General). Under s 9(5) of the *Director of Public Prosecutions Act*, the CDPP can take over a private prosecution and terminate it.

9.167 In its Inquiry into federal sedition laws, the ALRC raised concerns about the political nature of consent requirements.<sup>168</sup> Specifically, the Attorney-General, as a political figure, might be perceived to agree more readily to the prosecution of certain persons—such as those who criticise government policy or are unpopular with the electorate. Politicisation may also become an issue where the Attorney-General refuses consent—for example, to the prosecution of a person who is perceived to be politically aligned to the government of the day. As a consequence, the ALRC recommended removing the requirement for the Attorney-General’s consent to prosecution of sedition offences.<sup>169</sup> The Australian Government expressed support for this recommendation in its response to the ALRC report.<sup>170</sup>

### ***Submissions and consultations***

9.168 In IP 34, the ALRC asked whether the Attorney-General’s consent should be required for prosecutions under various secrecy provisions.<sup>171</sup>

9.169 In its submission, the AGD noted that:

Consent to prosecute provisions recognise the Attorney-General’s role as the First Law Officer and the Attorney-General’s ultimate responsibility for the prosecution of Commonwealth offences. Consent provisions give the Attorney-General a discretionary power to decide whether criminal proceedings should be commenced. The requirement for the Attorney-General’s consent is usually imposed where a prosecution could affect Australia’s international relations or national security. These are considerations which the Commonwealth Director of Public Prosecutions (CDPP) would not be able to take into account under the *Prosecution Policy of the Commonwealth*.

Consent provisions provide the Attorney-General with an opportunity to receive advice from relevant agencies on any sensitivities or issues which may arise if a prosecution is commenced. The Attorney-General’s consent may be appropriate in certain cases where there are matters of policy to be weighed up that are best left to elected representatives to decide. This might include consideration of whether there is potential for further damage to be done by airing the matter in court, or whether the prosecution could be detrimental to Australia’s foreign relations.<sup>172</sup>

9.170 The Australian Intelligence Community (AIC) stated that:

The AIC does not consider there has been any actual, or perceived, conflict of interest in the Attorney-General’s consent being required. Further, seeking the Attorney-General’s consent to prosecute ameliorates the potential strict application of these secrecy laws to the circumstances of an individual case.<sup>173</sup>

---

168 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Ch 13.

169 Ibid, Rec 13–1.

170 Australian Government, *Government Response to ALRC Review of Sedition Laws in Australia* (2008) <www.ag.gov.au> at 28 May 2009, response to Rec 13–1.

171 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–8.

172 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

173 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

9.171 In its submission, APRA noted that it is the CDPP, rather than the Attorney-General, who makes a decision whether or not to prosecute a breach of s 56 of the APRA Act and that this is broadly consistent with the position that decisions relating to prudential regulation should be made independently of the executive government.<sup>174</sup>

9.172 The Treasury expressed the view that:

It is important for the prohibition on the disclosure of taxpayer information to be clear and unambiguous. Therefore, in the absence of any uncertainty as to the application of the provisions, we do not consider that it would be appropriate for the Attorney-General's consent to be required.<sup>175</sup>

9.173 PIAC was opposed to the Attorney-General's gatekeeper role in relation to prosecutions for breach of Commonwealth secrecy laws, stating that:

The fact that such prosecutions involve material that government asserts should be kept secret, and the potential for party political considerations to intrude upon the decision-making process, makes such a role singularly inappropriate.<sup>176</sup>

#### *ALRC's views*

9.174 Section 8 of the *Director of Public Prosecutions Act 1983* (Cth) provides that the performance of the CDPP's functions is subject to directions or guidelines given by the Attorney-General. The Attorney-General can provide directions or guidelines about the circumstances in which the CDPP should institute or carry on prosecutions for offences, including in relation to particular cases. Such directions or guidelines must be published in the Australian Government *Gazette* and tabled in Parliament. The ALRC's view is that this is a more appropriate mechanism than a consent requirement. In particular, it ensures a level of transparency around any intervention in the prosecutorial decision making process by the Attorney-General.

9.175 As noted above, the ALRC expressed some concern in its report, *Fighting Words*, in relation to the requirement for the Attorney-General's consent to prosecution of sedition offences, and recommended the repeal of certain such requirements.<sup>177</sup> Given the Australian Government's support for this recommendation, the ALRC does not propose that the new general secrecy offence should include a requirement for the consent of the Attorney-General prior to the commencement of a prosecution under the provision.

#### **Infringement notices**

9.176 An infringement notice is a notice authorised by statute setting out the particulars of an alleged offence. It gives the person to whom the notice is issued the

---

174 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

175 The Treasury, *Submission SR 22*, 19 February 2009.

176 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

177 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Rec 13–1.

option of either paying the penalty set out in the notice or electing to have the matter dealt with by a court. Infringement notice schemes typically set penalties at 20% or less of the maximum fine that could be imposed by a court.

9.177 Infringement notices are not administrative penalties. Rather, they are an administrative device designed to dispose of a matter involving a breach that would otherwise have to be dealt with by a court—either by way of a criminal prosecution or in civil penalty proceedings.

9.178 To date, the ALRC has not identified any infringement notice schemes in Commonwealth secrecy provisions.<sup>178</sup> In *Principled Regulation: Federal Civil and Administrative Penalties in Australia (Principled Regulation)*, the ALRC recommended that in criminal penalty schemes, an infringement notice scheme should apply only to minor offences of strict or absolute liability.<sup>179</sup>

#### ***Submissions and consultations***

9.179 In IP 34, the ALRC asked whether infringement notice schemes had a role to play in enforcing breach of Commonwealth secrecy laws.<sup>180</sup>

9.180 Stakeholders were cautious about using infringement notices to enforce secrecy offences. In its submission, the AGD stated that:

An infringement notice scheme would not be appropriate for enforcing and punishing breaches of Commonwealth secrecy offences. Infringement notice schemes may be employed for minor offences, where a high volume of contraventions are expected, and where a penalty must be imposed immediately to be effective. None of these circumstances appear to be applicable when considering breaches of secrecy offences.<sup>181</sup>

9.181 ASIC noted that:

If an infringement notice scheme was to be introduced, then, in order to accord with the interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, the disclosure provisions to which the scheme applied would need to be framed so that:

- they only cover minor breaches; and

178 There are examples of infringement notice schemes in other areas of Commonwealth law. For example, infringement notices are alternative to civil penalty proceedings for alleged breach of continuous disclosure obligations: see *Corporations Act 2001* (Cth) pt 9.4AA. See also *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 497; *Migration Regulations 1994* (Cth) pt 5 div 5.5.

179 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Recs 12–1,12–2, 12–8. See also Recs 12–3 to 12–7. Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 51 also expresses the view that an infringement notice scheme should apply only to offences which do not require proof of fault and contain physical elements readily capable of assessment by an enforcement officer.

180 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–16.

181 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

- 
- no proof of fault element or state of mind is required.<sup>182</sup>

9.182 PIAC stated that:

PIAC does not believe an infringement notice regime is appropriate. Secrecy offences—certainly those that impose criminal liability—should not be offences of strict or absolute liability, as opposed to requiring proof of a fault element, or state of mind.<sup>183</sup>

#### ***ALRC's views***

9.183 The first tier general secrecy offence attaches strict liability to the requirement of proving that the unauthorised disclosure caused harm, or was reasonably likely to cause harm, to one of the specified public interests. However, the offence is still a serious one, given the requirement that the harm caused, or reasonably likely to be caused, is to significant public interests including national security, defence and international relations or the enforcement of the criminal law. The ALRC proposes that the first tier offence attract a maximum penalty of two years imprisonment.<sup>184</sup> As it is a serious criminal offence, enforcement by way of infringement notice is not appropriate.

9.184 The second and third tiers of the general secrecy offence and the subsequent disclosure offence are more serious offences involving recklessness, knowledge or intention to cause harm. They attract higher maximum penalties of five and seven years imprisonment, depending on the public interest harmed.<sup>185</sup> None of these offences could be described as ‘minor’ and, in the ALRC’s view, it would not be appropriate to enforce the provisions through an infringement notice scheme.

#### **Injunctions**

9.185 In some situations, the Australian Government may become aware that an unauthorised disclosure of Commonwealth information is about to occur. For example, information may have been leaked, and publication by the media or on an individual’s or organisation’s website appears imminent.

9.186 In *Keeping Secrets*, the ALRC analysed potential mechanisms to prevent disclosure of classified and security sensitive Commonwealth information in these circumstances.<sup>186</sup> The ALRC considered that injunctions to restrain a breach of the criminal law provided a potentially appropriate vehicle. However, in the absence of an

---

182 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

183 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

184 Proposal 9–3(a).

185 Proposal 9–3(b) and (c).

186 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Ch 5.

express statutory power, courts have traditionally been reticent to issue such injunctions.<sup>187</sup>

9.187 The right for the Attorney-General to invoke the aid of the civil courts in enforcing the criminal law has been described as one which 'is confined, in practice, to cases where an offence is frequently repeated in disregard of a usually inadequate penalty ... or to cases of emergency'.<sup>188</sup> In *Commonwealth v Fairfax*, Mason J further noted that:

It may be that in some circumstances a statutory provision which prohibits and penalizes the disclosure of confidential government information or official secrets will be enforceable by injunction. This is more likely to be the case when it appears that the statute, in addition to creating a criminal offence, is designed to provide a civil remedy to protect the government's right to confidential information.<sup>189</sup>

9.188 In the ALRC report, *Principled Regulation*, it was noted that injunctions are not in themselves penalties but are used in support of actions seeking penalties. In the course of that Inquiry, ASIC officers commented on the usefulness of injunctions in acting quickly against offenders:

The foundation of the ASIC approach is to try and protect investors, so the first step is always to act to protect, then start thinking about civil or criminal penalties.<sup>190</sup>

9.189 Section 17B of the *Taxation Administration Act 1953* (Cth) is an example of a provision that expressly provides for injunctive relief:

Where a person has engaged, is engaging or is proposing to engage in any conduct that constituted or would constitute a contravention of a taxation law that prohibits the communication, divulging or publication of information or the production of, or the publication of the contents of, a document, the Federal Court of Australia may ... grant an injunction restraining the person from engaging in the conduct ... requiring the person to do any act or thing.<sup>191</sup>

9.190 The Tax Laws Exposure Draft Bill also provides that, where someone is engaging, or proposing to engage, in breach of the new disclosure provisions, the Commissioner can apply to the Federal Court for an injunction.<sup>192</sup> The Explanatory Material to the Draft Bill provides the following example:

Jerome, a journalist, unlawfully obtains information regarding the financial affairs of a prominent businessman and decides to include that information in his newspaper the

187 See, eg, *Gouriet v Union of Post Office Workers* [1978] AC 435, 481, where Lord Wilberforce commented on the dangers of using the civil courts to impose injunctions, breach of which may attract criminal punishments.

188 *Ibid*, 481.

189 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50. Mason J held that s 79 of the *Crimes Act* was not such a provision.

190 Australian Securities & Investments Commission, *Consultation*, Sydney, 23 May 2001.

191 *Taxation Administration Act 1953* (Cth) s 17B(1).

192 Exposure Draft, *Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009* (Cth) sch 1, item 1, s 355-330.

following day. The Commissioner, who has become aware of this impending unlawful disclosure of taxpayer information, applies to the Federal Court for an injunction. The Federal Court issues an injunction against Jerome preventing him from publishing that information and also compelling him to return the information to the Australian Taxation Office (ATO).<sup>193</sup>

9.191 In *Keeping Secrets*, the ALRC noted the potentially compelling public interest in protecting classified and security sensitive information from unauthorised disclosure. The ALRC recommended that:

Sections 70 and 79 of the *Crimes Act 1914* (Cth) and s 91.1 of the *Criminal Code Act 1995* (Cth) should be amended to provide that, where the courts are satisfied that a person has disclosed or is about to disclose classified or security sensitive information in contravention of the criminal law, the courts may grant an injunction to restrain such disclosure or further disclosure.<sup>194</sup>

9.192 In IP 34, the ALRC asked whether secrecy laws should expressly provide for injunctions to restrain unauthorised disclosure of Commonwealth information and, if so, whether this should apply only to certain types of Commonwealth information, for example, national security or other sensitive Commonwealth information.<sup>195</sup>

### ***Submissions and consultations***

9.193 Stakeholders were generally supportive of providing the courts with power to issue injunctions to restrain the unauthorised disclosure of Commonwealth information. For example, the AGD's submission supported an express provision allowing the grant of such injunctions, but noted that:

On a practical level, it would be unlikely that there would be a significant number of cases where an injunction would be sought to protect unauthorised handling of Commonwealth information, as it is rare to have forewarning that unauthorised disclosure is likely to occur.<sup>196</sup>

9.194 APRA submitted that it would be useful to have an express power in s 56 of the APRA Act permitting APRA to obtain an injunction to prevent disclosure of material in breach of that provision.<sup>197</sup> The ATO noted that s 17B of the *Taxation Administration Act* expressly provides for injunctive relief and stated that:

The ATO considers this is a positive feature of tax secrecy provisions because it is preferable to obtain injunctive relief in relation to an unauthorised handling of taxpayer information, rather than seeking to pursue a criminal prosecution after the fact (at which point the information may already be in the public domain).<sup>198</sup>

---

193 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [7.8].

194 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–1.

195 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–4.

196 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

197 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

198 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

9.195 The Treasury agreed that the ability to obtain an injunction to prevent a breach of a taxation law forms an important part of the overall protection of taxpayer information:

Where possible, it can be used to prevent the damage caused (both to the individual and in the confidence in the tax system) which is preferable to punishing the conduct after the fact.<sup>199</sup>

9.196 The AIC supported the inclusion of ‘a statutory power to obtain injunctions to restrain unauthorised handling of national security-classified information’.<sup>200</sup> ASIC also expressed support noting that:

The availability of injunctions should not be limited to certain types of Commonwealth information. If Commonwealth information is regarded as being of such a nature as to warrant the coverage of secrecy provisions, whose aim is to deter and/or punish its unauthorised disclosure, then it should also warrant the protection of injunctions to prevent its disclosure. Prevention of unauthorised disclosure should be the key priority. If secrecy provisions are unsuccessful in achieving their desired deterrent effect, then injunctions will be the only remaining means of achieving the primary purpose of the secrecy provisions.<sup>201</sup>

9.197 PIAC agreed that:

where legislation prohibits and penalises the disclosure of Commonwealth confidential information, it is reasonable that it also provide a civil remedy, by way of injunctive relief, where disclosure would otherwise amount to a breach of the equitable duty of confidence. If the basis upon which an injunction might be obtained were governed by this principle, there is no apparent reason why it should be limited to national security, or other ‘sensitive’ information.<sup>202</sup>

9.198 Liberty Victoria sounded a note of caution, however:

The use of injunctive relief should be confined to [National Security Information]. An overly zealous approach to secrecy is counter to good government.<sup>203</sup>

#### ***ALRC’s views***

9.199 There was significant support among stakeholders for the inclusion of an express power to issue injunctions in secrecy offences. Although Liberty Victoria would limit the use of the power to restraining disclosure of national security information, the ALRC considers that this would be too narrow.

9.200 The proposed new general secrecy and subsequent disclosure offences are expressly limited to disclosures that involve actual or potential harm to the specific public interests discussed in Chapter 7. In the ALRC’s view, all these specific public

---

199 The Treasury, *Submission SR 22*, 19 February 2009.

200 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

201 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

202 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

203 Liberty Victoria, *Submission SR 19*, 18 February 2009.

interests merit the protection of the criminal law and should be further protected by granting the court the power to issue an injunction to restrain a breach of the provisions. Preventing disclosure of such information is a more effective mechanism to prevent the relevant harm than imposing a penalty after the damage is done. In considering whether to issue an injunction to restrain a breach of the provisions, the court will be required to consider the potential for harm to the listed public interests.

9.201 The ALRC proposes that the general secrecy offence, and the subsequent disclosure offence, should provide that, where a court is satisfied that a person has disclosed, or is about to disclose, information in contravention of the provisions, the court may grant an injunction to restrain such disclosure.

**Proposal 9–6** The proposed general secrecy offence, and the subsequent disclosure offence, should provide that, where a court is satisfied that a person has disclosed, or is about to disclose, information in contravention of the provisions, the court may grant an injunction to restrain such disclosure.

# 10. Specific Secrecy Offences: Elements

---

## Contents

Introduction	343
Reasonable likelihood of harm	344
Discussion	346
Submissions and consultations	347
ALRC's views	350
Fault element attaching to harm	352
Submissions and consultations	354
ALRC's views	355
Whose conduct should be regulated?	356
Submissions and consultations	358
ALRC's views	361
What conduct should be regulated?	362
Submissions and consultations	363
ALRC's views	364
Fault element attaching to disclosure	366
Submissions and consultations	367
ALRC's views	367
What information should be protected?	368
Submissions and consultations	369
ALRC's views	370

## Introduction

10.1 This chapter considers reform of specific secrecy criminal offence provisions—that is, secrecy offences other than ss 70 and 79(3) of the *Crimes Act 1914* (Cth), which have general application to Commonwealth officers and information.

10.2 As discussed in Chapter 6, the ALRC proposes that ss 70 and 79(3) of the *Crimes Act* be repealed and a new offence enacted in the *Criminal Code* (Cth) (the general secrecy offence). This new offence would be of general application to current and former Commonwealth officers in relation to the handling of information to which such officers have, or had, access to by reason of being officers.<sup>1</sup> In association, there would be an offence applying where any person knows that information has been

---

<sup>1</sup> Proposal 6–1.

disclosed by a Commonwealth officer in breach of the new general secrecy offence (the subsequent disclosure offence).<sup>2</sup>

10.3 This chapter, and Chapters 11 and 12, review specific secrecy offences in the light of the proposed general secrecy offence and the policy basis for that offence—an intention to promote more open government balanced against the need to protect Commonwealth information where unauthorised disclosure may cause harm to specified public interests. The aim of this exercise is to develop proposals to promote consistency in, and simplification of, Commonwealth secrecy offences.

10.4 These chapters highlight examples of where the scope of specific secrecy offences differs from the proposed general secrecy offence. While, in some cases, these differences are significant and necessary, specific secrecy offences should be framed more consistently with the policy of the general secrecy offence, and with each other. These chapters highlight aspects of the proposed general secrecy offence that might usefully be more broadly adopted.

10.5 The key elements of the offences considered in this chapter are: requirements for a reasonable likelihood of harm; the parties to offences; the relevant conduct; and the nature of the information protected. Chapter 11 conducts the same exercise with regard to exceptions, defences and penalties.

## **Reasonable likelihood of harm**

10.6 The proposed general secrecy offence would require that disclosure is reasonably likely to cause harm to specified public interests. As noted in Chapter 5, such a criterion is rarely incorporated into existing specific offence provisions.

10.7 A small number of secrecy offences, however, do incorporate a requirement of harm. For example:

- the ‘unauthorised disclosure of information’ offence in the *Defence Force Discipline Act 1982* (Cth) requires that a disclosure ‘is likely to be prejudicial to the security or defence of Australia’ in order for an offence to be committed;<sup>3</sup>
- the *Pooled Development Funds Act 1992* (Cth) protects information ‘the disclosure of which may reasonably be expected to affect a person adversely in respect of the lawful business, commercial or financial affairs of the person’;<sup>4</sup>

---

<sup>2</sup> Proposal 8–3.

<sup>3</sup> *Defence Force Discipline Act 1982* (Cth) s 58.

<sup>4</sup> *Pooled Development Funds Act 1992* (Cth) s 71(5).

- a secrecy offence in the *Aboriginal and Torres Strait Islander Act 2005* (Cth) refers to the disclosure of information ‘considered sacred or otherwise significant’ by a particular group of Aboriginal persons or Torres Strait Islanders where disclosure would be ‘inconsistent with the views or sensitivities of those Aboriginal persons or Torres Strait Islanders’;<sup>5</sup> and
- one of the ‘official secrets’ offences in the *Crimes Act*, requires that a communication be ‘with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen’s dominions’.<sup>6</sup>

10.8 As illustrated by these examples, a harm requirement may come in the form of an objective test or refer to the intention of the person making a disclosure, as in the case of the last example.

10.9 Further, the language used in some other secrecy provisions may make it clear that, in practice, the offences are directed to situations where harm to the public interests identified in the proposed general secrecy offence is anticipated. In particular, some offences define the relevant information or disclosure by reference, in part, to identifiable harms.

10.10 For example, the *Food Standards Australia New Zealand Act 1991* (Cth) provides that it is the duty of certain persons not to disclose ‘any confidential commercial information in respect of food’.<sup>7</sup> ‘Confidential commercial information’, for these purposes, is defined as:

- (a) a trade secret relating to food; or
- (b) any other information relating to food that has a commercial value that would be, or could reasonably be expected to be, destroyed or diminished if the information were disclosed.<sup>8</sup>

10.11 In many cases, the harm to which secrecy offences are aimed is implicit. For example, the secrecy offences contained in s 60 of the *Transport Safety Investigation Act 2003* (Cth) are aimed primarily at protecting the proper conduct of transport safety investigations. Arguably, the disclosure of ‘restricted information’, as defined in the Act,<sup>9</sup> would be reasonably likely to ‘prejudice the investigation of a breach of a law imposing a penalty or sanction’ in terms of the proposed general secrecy offence.

5      *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3).

6      *Crimes Act 1914* (Cth) s 79(2).

7      *Food Standards Australia New Zealand Act 1991* (Cth) s 114(1).

8      *Ibid* s 4(1). The meaning of ‘confidential commercial information’ is not always defined: eg, the *National Health and Medical Research Council Act 1992* (Cth) is stated to protect ‘confidential commercial information’ provided to National Health and Medical Research Council officers but the meaning of the term is not defined: see, *National Health and Medical Research Council Act 1992* (Cth) s 80.

9      *Transport Safety Investigation Act 2003* (Cth) ss 3, 60.

## Discussion

10.12 In Chapter 7, the ALRC proposes that, under the proposed general secrecy offence, the prosecution should be required to prove that a particular disclosure caused harm, was reasonably likely to cause harm, or was intended to cause harm to specified public interests, such as the national security, defence or international relations of the Commonwealth. In the absence of any actual, likely or intended harm to those public interests, the ALRC has formed the preliminary view that unauthorised disclosure of Commonwealth information is more appropriately dealt with by the imposition of administrative penalties or the pursuit of contractual or general law remedies.

10.13 There are arguments, however, that including a requirement to show harm would be inappropriate in the case of some specific secrecy offences. For example, in the case of intelligence and national security information, the Review of Commonwealth Criminal Law (Gibbs Committee) stated:

Undoubtedly, a member of the intelligence and security services stands in a special position and it is not unreasonable, in the opinion of the Review Committee, that he or she should be subject to a lifelong duty of secrecy as regards information obtained by virtue of his or her position ... the Review Committee is satisfied that disclosures by such persons should be prohibited by criminal sanctions without proof of harm.<sup>10</sup>

10.14 Such an approach is evident in ss 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth), which regulate the Australian Secret Intelligence Service (ASIS), the Defence Imagery and Geospatial Organisation (DIGO) and the Defence Signals Directorate (DSD) respectively. These secrecy provisions bind staff, contractors and others who interact with ASIS, DIGO and the DSD. They create offences for communicating information that was prepared by or on behalf of the organisations, connected with or relating to the performance of the organisations' functions. The provisions do not require that any such disclosure causes, is likely to cause or be intended to cause any harm to the public interest.<sup>11</sup> Rather, there is an implicit assumption that it is harmful to disclose such information.

10.15 Even in the area of national security information, however, not all commentators agree that a blanket prohibition should apply. While John McGinness notes that proof of disclosure will generally impose a less onerous burden on the prosecution than proof that disclosure will, or is likely to, cause harm, he expresses the view that:

One would hope that any reform in Australia ... would proceed on the basis that a test of harm resulting from disclosure should apply for even the most sensitive categories of national security and defence information.<sup>12</sup>

10.16 In the 2004 report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC recommended that a duty of secrecy

10 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 323.

11 The text of ss 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth) is set out in Appendix 3.

12 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 77.

should only be imposed in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm ‘the public interest’.<sup>13</sup>

10.17 Chapter 7 considers in detail which public interests justify the protection of secrecy provisions and examines the implications for the drafting of the proposed general secrecy offence. The concern in this chapter is about the extent to which it is desirable for specific secrecy offences to expressly include an element requiring that the unauthorised conduct have a reasonable likelihood of causing harm.

### Submissions and consultations

10.18 In the Issues Paper, *Review of Secrecy Laws* (IP 34), the ALRC asked whether all secrecy provisions should ‘expressly require that the unauthorised conduct cause, be likely to cause, or be intended to cause harm to a specified public interest’.<sup>14</sup>

10.19 This question provoked divergent responses from stakeholders, relevant both to the form of a general secrecy offence and to reform of specific secrecy offences. There were recurring themes, in relation to harm to public interests, which are also considered in detail in Chapter 7.

10.20 A number of stakeholders identified problems with the current lack of any requirement for harm in the drafting of most secrecy offences. For example, Ron Fraser stated that:

There are problems in the breadth of coverage of many provisions and their consequent lack of discrimination concerning the seriousness of a disclosure; their lack of reference (in most cases) to whether specific harm followed from disclosure, or could have been anticipated to follow, from disclosure of specific information; their application in some cases to material disclosure of which could be innocuous or of benefit to the public interest in some way ...<sup>15</sup>

10.21 The Public Interest Advocacy Centre (PIAC) considered that ‘the potential for harm should be a primary consideration in determining whether information should be treated as secret’. PIAC submitted that even information such as that relating to defence, or information held by the Australian Security Intelligence Organisation (ASIO), ‘should not be treated as secret if release or disclosure would not, and could not be reasonably expected to, harm specified public interests’.<sup>16</sup> In this regard, PIAC expressly opposed the approach taken by the Gibbs Committee.

---

13 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

14 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–7.

15 R Fraser, *Submission SR 42*, 23 March 2009.

16 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

10.22 The Law Council of Australia agreed that an element requiring that unauthorised conduct cause harm ‘would address concern about the broad scope of the current criminal secrecy provisions, which may capture disclosure of information that is already in the public domain or is otherwise innocuous’.<sup>17</sup> Similarly, the Australian Securities and Investments Commission (ASIC) stated that secrecy provisions should not ‘expose a person to liability for the disclosure of information which would be of minimal effect’ and should protect only ‘information that genuinely requires protection and/or that is likely to harm the public interest or a private interest’.<sup>18</sup>

10.23 Most agency stakeholders, however, opposed the incorporation of reasonable likelihood of harm requirements into specific secrecy offences.<sup>19</sup> The Australian Intelligence Community (AIC) stated that

a test of the harm—whether likely, intended or actual harm—to a specified public interest should not be a precondition for secrecy provisions relating to national security-classified information. The AIC notes that, in the first instance, the national security classifications applied to intelligence information are based on a measure of the possible level of harm likely to result from the unauthorised disclosure of that information. By way of example, a requirement to demonstrate harm would allow a person who releases the name of an ASIS officer to argue that they did not believe there was counter-intelligence value in the disclosed information and therefore there was no intent to harm the public interest.<sup>20</sup>

10.24 The AIC considered that individuals, within or outside the intelligence community, ‘should not be arbiters of which disclosures constitute damage to the public interest’. Such individuals are ‘not in a position to have an appropriate understanding or appreciation of the possible national security impact of releasing that information’.<sup>21</sup>

10.25 The Australian Prudential Regulation Authority (APRA) considered that the public interests being protected by the secrecy offences in the *Australian Prudential Regulation Authority Act 1998* (Cth)<sup>22</sup> (APRA Act) are implicit and, therefore, incorporating an express requirement for harm would be ‘unnecessary’.<sup>23</sup> The Australian Bureau of Statistics (ABS) referred to the secrecy offence in the *Census and Statistics Act 1905* (Cth)<sup>24</sup> and submitted that:

---

17 Law Council of Australia, *Submission SR 30*, 27 February 2009.

18 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

19 For example: Australian Intelligence Community, *Submission SR 37*, 6 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009; Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

20 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

21 Ibid.

22 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56.

23 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009. Also Department of Human Services, *Submission SR 26*, 20 February 2009.

24 *Census and Statistics Act 1905* (Cth) s 19.

The absolute nature of these provisions is its strength. If an approach were to be adopted that required proof of harm (etc), it would certainly have the impact of weakening (in both perception and reality) the ABS's ability to maintain the secrecy of identifiable information.<sup>25</sup>

10.26 Other agencies focused on the practical problems of incorporating a requirement of harm element into specific secrecy offences. The Australian Taxation Office (ATO) stated that this would be difficult 'as there may be no public interest reason not to disclose taxpayer information'<sup>26</sup>—that is, apart from the overall interest in maintaining taxpayer confidence in the privacy and confidentiality of information about them held by the ATO.

10.27 As noted in Chapter 7, the Commonwealth Director of Public Prosecutions (CDPP) considered that incorporating likelihood of harm requirements in secrecy offences would create difficulties for the prosecution.

Issues that would require attention would include, for example: who would give evidence of the harm to the specified public interest? Would that person need to be deemed to be an 'expert' so that s/he could give opinion evidence (and would the [Evidence Act 1995 (Cth)] need to be amended accordingly)? Would the act of giving such evidence cause further harm to the specified public interest?<sup>27</sup>

10.28 The Australian Government Attorney-General's Department (AGD) distinguished between secrecy offences dealing with different kinds of information. The AGD submitted that 'while harm to the public interest should be a key consideration and policy rationale for any secrecy provision, it may not be necessary to expressly include this as an element in all secrecy laws'. The AGD stated:

Some information may, by its very nature, be likely to cause harm, so it may not add much to include this as an element of the offence. Some examples may include intelligence information, defence information, information with a national security classification and Cabinet documents ... in these situations it should not be necessary for the prosecution to have to establish proof of harm.<sup>28</sup>

10.29 The AGD considered that, for information that is not 'by its very nature' likely to cause harm, it may be appropriate to 'link the offence to the public interest it is intended to serve in order to avoid the provision being unnecessarily broad'. The AGD concluded that a 'reasonably likely to cause harm' formulation would be a useful model for some secrecy offences.<sup>29</sup>

---

25 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

26 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

27 Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

28 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

29 Ibid.

### **ALRC's views**

10.30 As discussed in Chapter 7, there are a range of public interests that are capable of outweighing the public interest in open government. These interests form the policy rationale for the framing of the proposed new general secrecy offence so that an unauthorised disclosure of information must be reasonably likely to cause harm to one of those public interests in order to constitute a criminal offence.

10.31 This same policy rationale should form one starting point for the review of specific secrecy offences. In the ALRC's view, for an offence to be committed, there should generally be a reasonable likelihood that the disclosure of the information will cause harm to some important public interest. Where no such harm is likely, it is appropriate that the matter be subject only to administrative sanctions or contractual remedies, at least where the individual concerned is a Commonwealth officer.

10.32 Most existing specific secrecy offences, however, do not incorporate any such express requirement. For example, while many secrecy offences appear to be aimed primarily at protecting confidential commercial information held by government agencies from unauthorised disclosure, there is no express requirement that an unauthorised disclosure be reasonably likely to harm commercial interests.<sup>30</sup> It would be possible to incorporate in such offences a requirement that disclosure is reasonably likely to 'have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation'—to adopt the relevant clause of the proposed general secrecy offence.<sup>31</sup>

10.33 There are strong arguments, however, that in some contexts it would be inappropriate to include a reasonable likelihood of harm requirement. These contexts include situations where the likelihood of harm is self-evident, such as in relation to information held by the AIC.<sup>32</sup>

10.34 Section 18 of the *Australian Security Intelligence Organisation Act 1979* (Cth) creates an offence that applies where an officer or employee of ASIO communicates intelligence other than with the authority of the Director-General of ASIO. If a harm element were to be incorporated in this offence it might require, for example, that disclosure of information be proven 'reasonably likely to cause damage to the national

---

30 See, *National Health and Medical Research Council Act 1992* (Cth) s 80; *Pooled Development Funds Act 1992* (Cth) s 71(5).

31 See Proposal 7–1.

32 That is, the Office of National Assessments, ASIO, ASIS, the Defence Intelligence Organisation (DIO), DIGO and DSD. Existing secrecy offences that apply to the AIC were stated as: *Crimes Act 1914* (Cth) ss 70, 79; *Criminal Code* (Cth) s 91; *Australian Security Intelligence Organisation Act 1979* (Cth) ss 18, 34ZS, 81 and 92; *Intelligence Services Act 2001* (Cth) ss 39, 39A, 40, 41: Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

security, defence or international relations of the Commonwealth'—again, to adopt the relevant clause of the proposed general secrecy offence.<sup>33</sup>

10.35 As highlighted by the AIC, a harm requirement would allow a person to contest the intelligence significance of the information disclosed, presenting a significant barrier to successful prosecution.<sup>34</sup> Individual officers or others are not necessarily in a position to understand the significance of items of information to, for example, a foreign intelligence service. Predicting or assessing the likelihood of harm is extremely difficult in the context of security and intelligence information.

10.36 Arguably, imposing a requirement for harm in secrecy offences applying to AIC agencies would also be inconsistent with the current policy of the *Freedom of Information Act 1982* (Cth) (FOI Act), which exempts AIC agencies and documents from its operation. The Australian Government has indicated that this position will be retained under proposed reforms to the FOI Act, and exemptions will be extended to include the Defence Department 'in respect of its collection, reporting and analysis of operational intelligence and special access programs under which a foreign government provides restricted access to technologies'.<sup>35</sup>

10.37 Other examples of circumstances in which a likelihood of harm requirement would not be appropriate in secrecy offences are identified in the submissions discussed above. The ALRC is interested in further comment on this issue. In particular, many secrecy offences are seen as protecting interests in the effective operation of government—including the flow of information to, and within, government. Agencies may argue that, even where an unauthorised disclosure is not reasonably likely to have a 'substantial adverse effect on' personal privacy or commercial affairs—in terms of the proposed general secrecy offence—the disclosure may affect the willingness of the regulated community to provide information.

10.38 In some instances, it may be argued that the way in which specific secrecy offences are framed, and the context in which they operate, provide a sufficient likelihood that harm will be caused by an unauthorised disclosure and that an express requirement is unnecessary—for example, where the protected information is defined by reference to an identifiable harm.<sup>36</sup>

33 An alternative approach might be to limit the application of the offence to the disclosure of security classified information, on the basis that the classification process under the *Australian Government Protective Security Manual* involves consideration of whether damage may be caused to national security: Australian Government Attorney-General's Department, *Australian Government Protective Security Manual (PSM)* (2005).

34 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

35 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <[http://www.smos.gov.au/speeches/2009/sp\\_20090324.html](http://www.smos.gov.au/speeches/2009/sp_20090324.html)> at 24 March 2009.

36 As in the provisions discussed above: *Food Standards Australia New Zealand Act 1991* (Cth) s 4(1); *Pooled Development Funds Act 1992* (Cth) s 71(5).

10.39 Recognising these complexities, the ALRC considers that the incorporation of a reasonable likelihood of harm requirement should nevertheless be considered on a case-by-case basis as offences are reviewed, in accordance with the proposals in Chapter 12.<sup>37</sup> Such an approach is also consistent with the ALRC's proposal that s 38 of the FOI Act be repealed.<sup>38</sup>

**Proposal 10–1** Specific secrecy offences should generally incorporate a requirement that, for an offence to be committed, there must be a reasonable likelihood that the disclosure of information will cause harm to some specified public interest, except where there are clear countervailing public interests.

**Question 10–1** In what circumstances is it inappropriate for a secrecy offence to require that a disclosure be reasonably likely to cause harm—for example, in relation to the disclosure of national security classified information or information concerning the defence or international relations of the Commonwealth?

### Fault element attaching to harm

10.40 The proposed general secrecy offence would require the following fault elements attaching to harm:

- in the case of the first tier offence: strict liability,<sup>39</sup> so that no fault is required to be shown as to the likelihood of harm; and
- in the case of the other two tiers of the offence: recklessness, knowledge or intention as to the likelihood of harm.

10.41 The great majority of Commonwealth secrecy provisions do not stipulate fault elements. As discussed in Chapter 7, under the *Criminal Code*, where legislation creating an offence does not specify a fault element for a physical element consisting

---

37 Consistently with Proposal 7–3, it would also be appropriate, where a reasonable likelihood of harm requirement is incorporated in a specific secrecy offence, to consider whether there should be a defence applying in circumstances where the person can prove that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to cause the specified harm.

38 Proposal 4–1, and as recommended in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 70.

39 Under the *Criminal Code*, where strict liability applies to a particular physical element of the offence: (a) there are no fault elements for that physical element; and (b) the defence of mistake of fact under s 9.2 is available in relation to that physical element: *Criminal Code* (Cth) ss 6.1, 9.2.

of a circumstance or a result, the fault element is recklessness.<sup>40</sup> Under the Code, recklessness can be established by proving intention, knowledge or recklessness.<sup>41</sup>

10.42 In the secrecy offence context, a ‘circumstance’ will include, for example, that the information disclosed was acquired in the course of the person’s duties or is protected information, as defined by relevant provision. ‘Results’ are not often incorporated as an element in existing secrecy offences, but would include, for example, that the disclosure of the information causes harm.

#### **Circumstance or result**

10.43 Some specific secrecy offences specify that a fault element other than recklessness applies to a physical element consisting of a circumstance or a result. In most cases the fault element specified is knowledge relating to the nature of the information. For example:

- section 91B of the *Commonwealth Electoral Act 1918* (Cth) applies ‘if the person knows, or has reasonable grounds for believing, that the information has been obtained under section 90B’;
- section 114 of the *Development Allowance Authority Act 1992* (Cth) applies to a person who has commercial-in-confidence information because of performing duties or functions under the Act and knows that the information is commercial-in-confidence information; and
- section 323-50 of the *Private Health Insurance Act 2007* (Cth) applies where a person knows, or ought reasonably to know, that the disclosure to the person is not an authorised disclosure.

10.44 In other cases, specific secrecy offences provide that strict liability applies to a circumstance or result. For example:

- section 34ZS(3) of the *Australian Security Intelligence Organisation Act 1979* (Cth) provides that strict liability may apply to the circumstance that the information disclosed is ‘operational information’ as defined by the Act;
- section 58(3) of the *Child Support (Registration and Collection) Act 1988* (Cth) provides that strict liability applies to the circumstance that a disclosure or obtaining of information is a disclosure or obtaining for the purposes of pt IV of the Act; and

---

40 Ibid s 5.6(2).

41 Ibid s 5.4(4).

- section 204(3) of the *Social Security (Administration) Act 1999* (Cth) provides that strict liability applies to the circumstance under s 204(1) ‘that a person not authorised or required to do something is not authorised or required by or under the social security law or the *Farm Household Support Act 1992* to do that thing’.

### **Submissions and consultations**

10.45 In the AGD’s view, where difficulty arises in proving a fault element in relation to an offence, this usually relates to the fault element applicable to a circumstance or result. The AGD advised that:

It is current Commonwealth criminal law practice that strict or absolute liability should only be used in an offence where there are well thought out grounds for this. This reflects the basic premise that it is generally not in the interests of fairness or justice to subject people to criminal punishment for unintended actions or unforeseen consequences unless these resulted from an unjustified risk (ie recklessness). Strict liability should be introduced only after careful consideration on a case-by-case basis of all available options and should not be applied where the penalty for the offence includes imprisonment or where there is a monetary penalty greater than 60 penalty units.

Strict liability may be appropriate where it is necessary to ensure the integrity of a regulatory regime such as those relating to public health and safety, the environment, or financial or corporate regulation ... Absolute liability offences are rare and should be limited to jurisdictional or similar elements of offences that are not relevant to the person’s culpability.<sup>42</sup>

10.46 In relation to fault elements, the CDPP noted that:

it can be appropriate to apply absolute liability to a circumstance which links an offence to the legislative power of the Commonwealth (ie, the ‘Commonwealth connector’). For example, it would be appropriate to impose absolute liability to the circumstance in s 79(1)(b) [of the *Crimes Act*] that an official secret has been ‘entrusted to the person by a Commonwealth officer’ (Note: currently recklessness applies to this circumstance).<sup>43</sup>

10.47 The Treasury noted that some existing taxation secrecy offences contain elements to which strict liability applies. For example, under s 355-5(3) of sch 1 of the *Taxation Administration Act 1953* (Cth), strict liability is applied to the element of the offence that ‘the information was disclosed to you, or obtained by you, under an indirect tax law’.<sup>44</sup>

10.48 ASIC submitted that, if a reasonable likelihood of harm test were introduced into secrecy offences, strict liability should be applied to that element of the offences

---

42 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

43 Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

44 *Taxation Administration Act 1953* (Cth) sch 1, s 355-5(2)(c).

'because it would be very difficult to prove that a person intended or knew that, their disclosure was likely to harm a specified public interest'.<sup>45</sup>

### ALRC's views

10.49 In the ALRC's view, where specific secrecy offences incorporate a reasonable likelihood of harm requirement, the same fault elements should apply as under the proposed general secrecy offence.

10.50 For offences punishable by imprisonment for more than a maximum of two years, recklessness, knowledge or intention should generally be the fault elements. For other offences, strict liability should apply to the likelihood of harm. That is, a person need not be reckless as to the likelihood of harm, know that harm might result, or intend harm in order to attract criminal liability for an unauthorised disclosure.

10.51 Some specific secrecy offences stipulate that strict liability applies to some other physical element consisting of a circumstance or a result. For example, as noted above, s 58 of the *Child Support (Registration and Collection) Act 1988* (Cth) provides that strict liability applies to the circumstance that a disclosure or obtaining of information is for the purposes of pt IV of the Act. Part IV deals with the collection of child support payments by employer deduction from salary or wages. The secrecy offence in s 58 applies to the employers who make, or are liable to make, withholding payments, and to their employees.

10.52 The application of strict liability ensures that the prosecution is not required to prove that an employer or employee knew or was reckless as to whether, for example, the information was originally obtained in order to ensure that periodic amounts payable by a parent towards the maintenance of child are made. Such a position may be justifiable, because a person's knowledge of such matters would be difficult for the prosecution to prove, and it may be considered sufficient that a defence of honest and reasonable mistake of fact is available to the defendant under the *Criminal Code*.<sup>46</sup>

**Proposal 10–2** (a) Where specific secrecy offences incorporate a reasonable likelihood of harm requirement, recklessness should generally be the fault element for offences punishable by imprisonment for more than a maximum of two years.

(b) For other offences, strict liability should apply in relation to the likelihood of harm.

45 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

46 *Criminal Code* (Cth) ss 6.1(2), 9.2.

## **Whose conduct should be regulated?**

10.53 The proposed general secrecy offence would apply to current and former ‘Commonwealth officers’. For these purposes, a Commonwealth officer is defined to include: individuals appointed or engaged under the *Public Service Act 1999* (Cth); individuals employed by the Commonwealth otherwise than under the *Public Service Act*; individuals who hold or perform the duties of an office established by or under a law of the Commonwealth; officers or employees of Commonwealth authorities; individuals and entities who are contracted service providers for a Commonwealth contract; and individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth.<sup>47</sup>

10.54 There is considerable variation in the way in which the parties subject to specific secrecy offences are described. Secrecy provisions are stated to apply variously to Commonwealth officers; other individuals providing services for, or on behalf of, the Commonwealth; other specific categories of individual; or any person.

10.55 At present, around 35% of Commonwealth secrecy provisions (about 130 offences) regulate the activities of categories of Commonwealth officer. These offences may apply to:

- all Commonwealth officers;<sup>48</sup>
- all officers of specific Commonwealth agencies;<sup>49</sup> and/or
- specific agency heads or officers.<sup>50</sup>

10.56 Most of these offences (about 75%) regulate the activities of former, as well as current, Commonwealth officers—for example, by protecting information acquired by a person ‘by reason of his or her being, or having been, an officer or employee’ of an agency.<sup>51</sup>

10.57 Around 15% of secrecy offences extend to individuals providing services for or on behalf of the Commonwealth.<sup>52</sup> In addition, individuals engaged in federally funded

47 See Proposal 8–1.

48 For example, *Income Tax Assessment Act 1936* (Cth) s 16.

49 For example, *Australian Postal Corporation Act 1989* (Cth) ss 90H, 90LB apply to ‘employees of Australia Post’; *Customs Administration Act 1985* (Cth) s 16 applies to ‘a person performing duties in the Australian Customs Service as a person employed or engaged by the Commonwealth, a Commonwealth agency, a State or a State agency’.

50 For example, *National Health and Medical Research Council Act 1992* (Cth) s 80(7) applies to the Chief Executive Officer of the National Health and Medical Research Council and the Commissioner of Complaints.

51 For example, *Australian Security Intelligence Organisation Act 1979* (Cth) s 18.

52 For example, *Australian Sports Anti-Doping Authority Act 2006* (Cth) s 69 (definition of ‘entrusted person’), s 72; *Australian Trade Commission Act 1985* (Cth) s 62 (definition of ‘consultant’), s 94.

or regulated areas of the private sector—for example, health service providers<sup>53</sup> and employees of financial institutions<sup>54</sup>—may also be subject to secrecy provisions. Some secrecy provisions extend to state and territory government employees and local government employees—for example, to facilitate information transfer between federal and state taxation authorities.<sup>55</sup>

10.58 A diverse range of other individuals are regulated by Commonwealth confidentiality or secrecy provisions. These include:

- individuals assisting in epidemiological studies;<sup>56</sup>
- individuals assisting transport security inquiries;<sup>57</sup>
- Pharmaceutical Benefits Scheme prescribers;<sup>58</sup>
- participants in witness protection programs;<sup>59</sup> and
- legal practitioners representing persons involved in Australian Crime Commission examinations.<sup>60</sup>

10.59 More than 40% of secrecy offences are stated to apply to the handling of information by ‘any person’. An example is s 79 of the *Crimes Act*, which prohibits unauthorised handling or communication of official secrets by any person, including members of the media.

#### ***Initial and subsequent disclosures***

10.60 The respective scope of the proposed general secrecy offence and specific secrecy offences with regard to the parties covered must be considered in conjunction with provisions that extend the coverage of offence provisions to subsequent disclosures.

10.61 The proposed subsequent disclosure offence would provide that, where a person knows, or is reckless as to whether: information has been disclosed by a Commonwealth officer in breach of the general secrecy offence; and the subsequent disclosure of the information will harm, or is reasonably likely to harm, one of the

---

53     *National Health Act 1953* (Cth) s 135AAA.

54     *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 123.

55     *Taxation Administration Act 1953* (Cth) s 13J.

56     *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 4.

57     *Inspector of Transport Security Act 2006* (Cth) s 35(7).

58     *National Health Act 1953* (Cth) s 135AAA(1).

59     *Witness Protection Act 1994* (Cth) s 22(2).

60     *Australian Crime Commission Act 2002* (Cth) s 29B(4).

specified public interests, disclosure of that information by that person is also an offence.

10.62 About 30% of secrecy offences extend to some form of subsequent disclosure. For example, s 8XB(1) of the *Taxation Administration Act 1953* (Cth) provides that a person ‘shall not directly or indirectly ... divulge or communicate to another person any taxation information relating to a third person ... being information disclosed to or obtained by the person in breach of a provision of a taxation law (including this provision)’.

10.63 As with the subsequent disclosure offence, the *Taxation Administration Act* provision deals with disclosure of information received as a result of a breach of a secrecy law. Other provisions deal with subsequent disclosure where the information was obtained legally. For example, under s 86-5 of the *Aged Care Act 1997* (Cth) it is an offence to disclose protected information disclosed by the Secretary for a purpose other than that for which the information was originally disclosed.

### **Submissions and consultations**

10.64 In IP 34, the ALRC asked in what circumstances should secrecy provisions regulate the behaviour of persons other than core Commonwealth officers such as: consultants and others who provide goods and services to the Australian Government; those who enter into arrangements with the Australian Government; and state and territory government employees.<sup>61</sup>

10.65 The ALRC also asked:

- when should secrecy provisions regulate the behaviour of ‘any person’;<sup>62</sup>
- in what circumstances should secrecy provisions regulate those who have been but who are no longer Commonwealth officers;<sup>63</sup> and
- whether all secrecy provisions should seek to regulate both initial and subsequent unauthorised handling of Commonwealth information.<sup>64</sup>

10.66 Many stakeholders referred to the need for specific secrecy offences to apply to parties other than Commonwealth officers.<sup>65</sup> The Department of Human Services (DHS), for example, submitted that:

---

61 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–1.

62 Ibid, Question 3–2.

63 Ibid, Question 3–3.

64 Ibid, Question 3–5.

65 For example, Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

it is important that staff (including contracted staff and staff of contracted service providers (CSPs) and partners such as state governments, NGOs and the private sector) working for or with agencies and handling customer information, appreciate the personal nature of their obligation to protect the confidentiality of a range of information entrusted to the agency. A secrecy provision that creates an offence applying directly to individual employees is an effective tool for reinforcing this message.<sup>66</sup>

10.67 The DHS noted that, while the *Public Service Act* provides ‘a mechanism for holding individual Australian Public Service employees responsible for their behaviour, including unlawful dealing with information’, the Act

does not apply to other people who may come into possession of sensitive information (for example, [contracted service providers] and their employees, ministerial staff, State, NGOs and private sector partners and those who receive information in error).<sup>67</sup>

10.68 The ATO emphasised the importance of secrecy provisions regulating ‘all persons, who in the context of employment or performing services for the Commonwealth, come into contact with protected information’ and that protected tax information that is disclosed to a state or territory government employee remains protected by the tax law secrecy provision under which it was disclosed.<sup>68</sup>

10.69 Most stakeholders who addressed the issue considered that specific secrecy offences should generally extend to former Commonwealth officers and that, if this were not the case, it would significantly undermine the utility of secrecy provisions.<sup>69</sup> For example, APRA stated that:

Former officers may no longer be bound by duties of confidentiality contained in employment agreements and therefore a statutory secrecy provision may often be the only means of protecting the disclosure of information that the person had access to during their employment ...

In APRA’s case, staff who leave the agency may do so to take up employment with a financial sector entity, and in these circumstances it is particularly important that information they have obtained during the course of their employment with APRA be kept secret.<sup>70</sup>

---

66 Department of Human Services, *Submission SR 26*, 20 February 2009.

67 Ibid.

68 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

69 Australian Intelligence Community, *Submission SR 37*, 6 March 2009; NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

70 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

10.70 Stakeholders also highlighted the need for subsequent disclosure provisions. The Treasury stated that provisions such as that in s 8XB of the *Taxation Administration Act*, ‘continue to be appropriate to ensure the integrity of information and the integrity of authorised chains of disclosure’.<sup>71</sup>

10.71 Under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act), the Australian Transaction Reports and Analysis Centre (AUSTRAC) may disseminate AUSTRAC information to designated agencies and other persons, including state and territory government agencies and Royal Commissions of Inquiry. The AML/CTF Act prohibits the disclosure of AUSTRAC information by designated agencies, subject to a range of exceptions.<sup>72</sup> AUSTRAC submitted that:

State and Territory Government agencies which access AUSTRAC information should be subject to the same disclosure provisions as Australian Government agencies, given that disclosure of AUSTRAC information may not be in the public interest or might be harmful to individuals or persons that are the subject of reports ... or that are reporting entities or cash dealers under those pieces of legislation.<sup>73</sup>

10.72 The Australian Federal Police (AFP) stated that secrecy offences should cover subsequent use of information in circumstances where a person ‘should reasonably be aware that the information they have obtained was, at some point, disclosed on an unlawful basis and/or is classified or protected and should not be further used or disseminated’. This type of provision was said to be

particularly necessary in the spheres of criminal investigations and national security where the disclosure of information can compromise a serious investigation, threaten the security of the Commonwealth and diminish the confidence that Government holds in its agencies. Breaches of secrecy laws in these spheres have serious, long lasting effects irrespective of whether they are coupled with potential immediate consequences to life, property, and ongoing operations.<sup>74</sup>

10.73 Similarly, the Australian Commission for Law Enforcement Integrity (ACLEI) stated that:

ACLEI has a concern about inappropriate associations between current and former staff of law enforcement agencies, including where the former officer acts as an intermediary for criminals. ACLEI notes that the same damage, and sometimes more, can result from a secondary disclosure as it can from the primary disclosure.

Accordingly, ACLEI believes that the criminalisation of ‘subsequent unauthorised disclosure’ would be a valuable deterrent against corrupt (intentional) disclosure.<sup>75</sup>

---

<sup>71</sup> The Treasury, *Submission SR 22*, 19 February 2009.

<sup>72</sup> *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 128.

<sup>73</sup> Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

<sup>74</sup> Australian Federal Police, *Submission SR 33*, 3 March 2009.

<sup>75</sup> Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

10.74 The DHS noted that one advantage of subsequent disclosure provisions is that they extend the ‘lifespan and consistency of the protection of the secrecy law to the information in the hands of a third party’.

In the absence of secondary obligations, there will be different rights and obligations applying to identical information depending on whose hands it is in. This diminishes the level of protection warranted to the person whose information is concerned when that information was collected or created. Human services agencies typically ensure that any contract for services where sensitive information will be exchanged contains a clause requiring the [contracted service provider] to abide by the agency’s secrecy provision, whether or not the contractor is legally bound by that provision under the terms of the Act. However, the position with potential partners such as state governments, NGOs and private sector entities, is not clear particularly where they may already be subject to (legislative) regulation of their own which is at variance with the agency’s secrecy laws.<sup>76</sup>

### ALRC’s views

10.75 The general secrecy offence applies to current and former Commonwealth officers, including Commonwealth service providers. The subsequent disclosure offence extends the reach of criminal sanctions to persons who know, or are reckless as to whether, information has been disclosed in breach of the general secrecy offence.

10.76 Specific secrecy offences apply to categories of person that are both broader and narrower than those covered by the proposed general secrecy offence and subsequent disclosure offence.

10.77 Many existing secrecy offences apply to parties other than Commonwealth officers. The ALRC estimates that around 70% of existing secrecy offences (about 245 offences) apply to some parties who do not fall within the extended definition of Commonwealth officer contained in the proposed general secrecy offence.

10.78 In many cases, the need to cover other individuals as potential parties to an offence is clearly justifiable, as with some secrecy offences contained in the *Crimes Act*, which apply to ‘any person’.<sup>77</sup> In other cases, secrecy offences need to cover specific categories of individuals, such as participants in witness protection programs,<sup>78</sup> or legal practitioners.<sup>79</sup>

10.79 However, the language used in some secrecy offences, and the practical context in which the provisions operate, mean that the provisions will apply mainly to Commonwealth officers—even if the offences are stated to apply to ‘any person’. For

---

76 Department of Human Services, *Submission SR 26*, 20 February 2009.

77 For example, *Crimes Act 1914* (Cth) ss 15XS, 79.

78 *Witness Protection Act 1994* (Cth) s 22(2).

79 *Australian Crime Commission Act 2002* (Cth) s 29B.

example, the information protected by such provisions is often defined as information ‘acquired by the person in the course of performing duties or exercising powers or functions’ under certain legislation;<sup>80</sup> or as information obtained for the purposes of certain legislation and held in the records of specific agencies.<sup>81</sup>

10.80 In the ALRC’s view, specific secrecy offences that are stated to apply to ‘any person’ should be reviewed to establish whether the offences should apply only to ‘Commonwealth officers’ and subsequent disclosure, as these are defined in the general secrecy offence and the subsequent disclosure offence respectively.

10.81 Specific secrecy offences that apply to Commonwealth officers should also be reviewed to establish whether the offences should be stated to apply to both former and current Commonwealth officers. As discussed in Chapter 8, in the case of the proposed general secrecy offence, the requirement that any disclosure must cause harm, be reasonably likely to cause harm, or be intended to cause harm, will limit the practical application of the offence to former Commonwealth officers. As discussed above, most existing specific secrecy offences, do not incorporate any such express requirement for harm—although the ALRC has proposed that offences should generally do so.<sup>82</sup> The existence, or otherwise, of a harm requirement is one factor that should be taken into account in reviewing this aspect of specific secrecy offences.

**Proposal 10–3** Specific secrecy offences that are stated to apply to ‘any person’ should be reviewed to establish whether the offences should apply only to ‘Commonwealth officers’ and to subsequent disclosure, as defined in the general secrecy offence and the subsequent disclosure offence (Proposals 8–1, 8–3).

**Proposal 10–4** Specific secrecy offences that apply to Commonwealth officers should be reviewed to establish whether the offences should be stated to apply also to former Commonwealth officers.

## What conduct should be regulated?

10.82 The conduct covered by the proposed general secrecy offence is the ‘disclosure’ of information. As discussed in Chapter 5, 90% of secrecy provisions prohibit disclosing, divulging or communicating Commonwealth information. A similar proportion of specific secrecy offences (85%) prohibit this kind of conduct. In addition,

<sup>80</sup> For example, *Aged Care Act 1997* (Cth) s 86-2.

<sup>81</sup> For example, *Student Assistance Act 1973* (Cth) ss 353, 3(1) (definition of ‘protected information’).

<sup>82</sup> See Proposal 10–2.

some secrecy offences prohibit unauthorised soliciting,<sup>83</sup> or receipt,<sup>84</sup> of information, as well as obtaining,<sup>85</sup> possessing,<sup>86</sup> making a record of,<sup>87</sup> or using<sup>88</sup> information.

10.83 As discussed in Chapter 8, around 60% of Commonwealth secrecy offences cover conduct other than (and usually in addition to) the disclosure of information. Most commonly, the other conduct involves ‘making a record’ of information (found in around 40% of offences).<sup>89</sup> A few existing secrecy offences criminalise the mere possession or receipt of information.<sup>90</sup>

### Submissions and consultations

10.84 In IP 34, the ALRC asked whether it is appropriate for secrecy provisions to regulate conduct other than the disclosure of information—such as the unauthorised receipt, collection, use or recording of information.<sup>91</sup> Stakeholders made comments relevant to the scope of specific secrecy offences, as well as to the formulation of the proposed general secrecy offence.

10.85 For example, a number of stakeholders submitted that secrecy offences in their areas of interest should extend beyond the disclosure of information. The AIC stated that it supported

the current formulation of s 91.1 of the *Criminal Code* which prohibits collection and recording of information. This formulation provides scope to prevent espionage activities or possible unauthorised disclosures of national security-classified information that would not be possible if the provision was limited to the disclosure itself. Without the current formulation, a person could only be prosecuted after they had committed the act of espionage or unauthorised disclosure of information. By that time, any damage to national security would have occurred.<sup>92</sup>

10.86 The Department of Education, Employment and Workplace Relations (DEEWR) also focused on the need to prevent harm, whether caused by disclosure or other conduct, such as access to departmental databases by staff members for personal reasons.<sup>93</sup>

---

83 For example, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 165.

84 For example, *Crimes Act 1914* (Cth) s 79(6).

85 For example, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 163.

86 For example, *Defence (Special Undertakings) Act 1952* (Cth) s 9(2).

87 For example, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.

88 For example, *Aged Care Act 1997* (Cth) s 86-5.

89 For example, *Criminal Code* (Cth) s 91.1(3).

90 *Crimes Act 1914* (Cth) ss 79(4)-(6), 83; *Defence (Special Undertakings) Act 1952* (Cth) s 9(2).

91 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3-4.

92 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

93 Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009. DEEWR also noted that ‘greater clarity between what constitutes a use as opposed to a disclosure of information would be useful’.

10.87 The ATO submitted that the access, use, recording and disclosure of information should be subject to secrecy provisions.<sup>94</sup> The Treasury stated that recording, as well as disclosure, should be covered and that there may be circumstances when other conduct, such as accessing information, should also fall within the ambit of specific secrecy offences.<sup>95</sup> In this context, the ATO and Treasury both noted that s 8XA of the *Taxation Administration Act 1953* (Cth) provides that a person ‘must not take action with the intention of obtaining’ taxation information about another person.<sup>96</sup> ASIC submitted that secrecy offences should extend to use, disclosure or recording.<sup>97</sup>

10.88 Other stakeholders accepted that it may be sufficient to proscribe disclosure, rather than other aspects of information-handling.<sup>98</sup> In this context, the DHS noted that:

Relevant agencies, including Medicare Australia, suggest that the absence of a prohibition on use causes no practical difficulties as other sanctions (including under the *Public Service Act* and the *Privacy Act*) apply to unauthorised collection and use.<sup>99</sup>

10.89 In relation to the conduct that should be covered by secrecy provisions, the AGD observed that:

The conduct that should be regulated by secrecy provisions will depend upon the policy rationale and harm sought to be avoided. If harm can be caused by unauthorised handling, access or use of information, then it would seem appropriate for these actions to also be prohibited.<sup>100</sup>

### **ALRC’s views**

10.90 In the ALRC’s view, the focus of secrecy offences should be on the unauthorised disclosure of Commonwealth information. As discussed in Chapter 8, some other activity, where it is ancillary to the primary offence, will be covered by other provisions in the *Criminal Code*. These extensions of criminal responsibility include attempt, aiding, abetting, procuring, incitement and conspiracy.<sup>101</sup> Criminal responsibility will, therefore, extend to much activity that is preliminary to disclosure. For example, the offence of incitement may apply where a third party solicits the unauthorised disclosure of information from a Commonwealth officer.<sup>102</sup>

10.91 Further, other provisions of the *Criminal Code* apply to the unauthorised use of, or access to, Commonwealth information. For example, the use of information is

---

94 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

95 The Treasury, *Submission SR 22*, 19 February 2009.

96 Ibid; Australian Taxation Office, *Submission SR 13*, 16 February 2009.

97 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

98 Law Council of Australia, *Submission SR 30*, 27 February 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

99 Department of Human Services, *Submission SR 26*, 20 February 2009.

100 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

101 See *Criminal Code* (Cth) pt 2.4.

102 See *Ibid* s 11.4.

covered by the provisions dealing with abuse of public office.<sup>103</sup> Unauthorised access to, or modification of, data where held in a Commonwealth computer, is also the subject of existing offence provisions.<sup>104</sup>

10.92 In some specific contexts it might be considered appropriate to criminalise other aspects of unauthorised information-handling. The majority of taxation secrecy provisions contained in the exposure draft Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill, released by Treasury in March 2009 (Tax Laws Exposure Draft Bill), refer to both the disclosure and recording of taxpayer information.<sup>105</sup> That is, it would be an offence to ‘make a record’ of information. The explanatory material to the Tax Laws Exposure Draft Bill provides the following rationale:

The offence provisions apply not only to the disclosure of taxpayer information, but also to the recording of that information. This recognises that it is important not only to ensure that information is not disclosed unlawfully, but that the information is not recorded in another form that can be readily accessed by others.<sup>106</sup>

10.93 An example of the potential application of this offence is also provided:

In the course of her duties as a taxation officer, Stacey found herself working with the taxation files of a musical artist whom she very much admired. Stacey copied some details from the taxation files into her private diary. Even though Stacey has not disclosed that information, she has still committed an offence through the recording of the information.<sup>107</sup>

10.94 The ALRC is not convinced that it is appropriate for such conduct to constitute a criminal offence—administrative sanctions may be sufficient. It is easier, however, to argue in favour of such an offence in relation to information contained in taxation files than is the case with some other information. For example, under s 60 of the *Age Discrimination Act 2004* (Cth), it is an offence for a member of the staff of the Australian Human Rights Commission to ‘make a record of’ any information ‘relating to the affairs of another person’ acquired because of their employment. The harm involved in such conduct is not immediately obvious and administrative action may provide an adequate sanction.

10.95 In the ALRC’s view, specific secrecy offences that extend to conduct other than the disclosure of information should be reviewed to establish whether this is necessary or desirable.

---

103 Ibid s 142.2.

104 Ibid ss 477.1, 478.1.

105 See, eg Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 paras 355-20(1)(b)(i), 355-155(1)(a)(i), 355-265(1)(a). Unauthorised access to taxpayer information will also continue to be an offence under the *Taxation Administration Act 1953* (Cth) s 8XA.

106 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), 24.

107 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), 24.

**Proposal 10–5** Specific secrecy offences should generally not extend to conduct other than the disclosure of information, such as making a record, receiving or possessing protected information.

### Fault element attaching to disclosure

10.96 The proposed general secrecy offence would require intention as to the disclosure of information.

10.97 As noted in Chapter 8, the great majority of Commonwealth secrecy offences do not stipulate fault elements. Under the *Criminal Code*, where legislation creating an offence does not specify a fault element for a physical element consisting of conduct, the fault element is intention.<sup>108</sup> In the secrecy offence context, the relevant ‘conduct’ will usually be the disclosing, divulging or communicating of information.

10.98 The fault element for the conduct elements of almost all specific secrecy offences (around 95%) is intention. In most cases, this is because no fault element is specified and, therefore, the *Criminal Code* provides that intention is required, reflecting the common law.

10.99 Only a few existing specific secrecy offences specify that some fault element other than intention applies to the disclosure or other handling of information. For example:

- under s 23YO(1)(c) of the *Crimes Act*, a person is guilty of an offence if the person is reckless as to the disclosure of information stored on the Commonwealth DNA database system or National Criminal Investigation DNA Database or any other information revealed by a forensic procedure carried out on a suspect, offender or volunteer; and
- under s 3ZQJ of the *Crimes Act*, a person is guilty of an offence if the person is reckless as to the disclosure of age determination information.

10.100 Some other specific secrecy offences provide that strict liability applies to the relevant conduct. That is, there are no fault elements for any of the physical elements of the offence and the defence of mistake of fact is available.<sup>109</sup> For example, s 63(2) of the *Superannuation (Resolution of Complaints) Act 1993* (Cth), provides that certain persons must not disclose any information acquired in connection with a

---

<sup>108</sup> *Criminal Code* (Cth) s 5.6(1).

<sup>109</sup> Ibid ss 6.1, 9.2.

complaint made to the Superannuation Complaints Tribunal. This offence is stated to be an offence of strict liability.<sup>110</sup>

### Submissions and consultations

10.101 The AGD emphasised that ‘the fault elements supplied by the *Criminal Code* should apply unless there is a justifiable reason for departing from them’, although strict liability ‘may be appropriate’

where it is necessary to ensure the integrity of a regulatory regime such as those relating to public health and safety, the environment, or financial or corporate regulation ... Absolute liability offences are rare and should be limited to jurisdictional or similar elements of offences that are not relevant to the person’s culpability.<sup>111</sup>

10.102 The Law Council of Australia stated that it has concerns about the introduction of strict liability or absolute liability<sup>112</sup> offences ‘without substantial evidence that such liability is warranted and there seems little such evidence in the context of criminal secrecy provisions’.<sup>113</sup>

10.103 Treasury stated that, in its consideration of the consolidation of taxation secrecy provisions, there had not been ‘any reason to depart from the default provisions of the *Criminal Code*'.<sup>114</sup> That is, imposing strict liability was not considered necessary. The Tax Laws Exposure Draft Bill does not apply strict liability to any element of the equivalent offences.<sup>115</sup>

### ALRC’s views

10.104 The ALRC proposes that the new general secrecy offence should require intention as to the disclosure of information. This is consistent with the framing of most existing secrecy offences, and with the policy reflected by the *Criminal Code*.

10.105 However, as discussed in Chapter 8, there are some reasons to suggest that—given the incorporation of a reasonable likelihood of harm test in the proposed general secrecy offence—recklessness as to disclosure should be sufficient. That is, because the reasonable likelihood of harm requirement substantially narrows the scope of the

---

110 *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63(2A).

111 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

112 Under the *Criminal Code*, absolute liability applies where there are no fault elements for any of the physical elements of the offence; and the defence of mistake of fact is unavailable: *Criminal Code* (Cth) ss 6.2, 9.2.

113 Law Council of Australia, *Submission SR 30*, 27 February 2009.

114 The Treasury, *Submission SR 22*, 19 February 2009. Consolidation of taxation secrecy provisions is discussed in more detail in Ch 12.

115 Exposure Draft, *Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009* (Cth) sch 1 pt 1 paras 355-20, 355-155.

offence—as compared with the existing offence in s 70 of the *Crimes Act*—recklessness may be considered an appropriate fault element.

10.106 If the general secrecy offence were to apply where a person was reckless as to disclosure, questions would arise about whether specific secrecy offences should be framed in the same way, at least where specific offences also incorporate a reasonable likelihood of harm requirement.

10.107 Some existing offences apply strict liability to physical elements dealing with conduct. For example, s 63 of the *Superannuation (Resolution of Complaints) Act 1993* (Cth) applies strict liability to an offence involving the disclosure of superannuation complaint information. In the ALRC's view, specific secrecy offences that provide that strict liability applies to one or all physical elements should be reviewed to establish whether the application of strict liability remains justified.

**Proposal 10–6** Specific secrecy offences should generally require intention as the fault element for the disclosure of information.

**Proposal 10–7** Specific secrecy offences that provide that strict liability applies to one or all physical elements should be reviewed to establish whether the application of strict liability remains justified.

## What information should be protected?

10.108 The proposed new general secrecy offence potentially applies to all information to which a Commonwealth officer has, or had, access to by reason of being a Commonwealth officer. In contrast, most specific secrecy offences prohibit the unauthorised handling of specific categories of Commonwealth information. These include, for example, offences that relate to the disclosure of:

- personal information,<sup>116</sup> or information concerning or relating to the affairs of another person;<sup>117</sup>
- confidential information—including confidential commercial information,<sup>118</sup> and other information that is supplied in confidence.<sup>119</sup>

<sup>116</sup> See, eg, *Higher Education Support Act 2003* (Cth) s 179-10, sch 1 (definition of ‘personal information’); *Aged Care Act 1997* (Cth) s 86-2(1).

<sup>117</sup> *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3)(a); *A New Tax System (Australian Business Number) Act 1999* (Cth) ss 30, 41; *Income Tax Assessment Act 1936* (Cth) s 16(2).

<sup>118</sup> For example, *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s 162(1); *Gene Technology Act 2000* (Cth) s 187.

<sup>119</sup> For example, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32; *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) ss 604-15, 604-20.

- defence or security information—information the unauthorised disclosure of which may prejudice defence or security;<sup>120</sup>
- law enforcement and intelligence information—information about the operations or investigations of law enforcement agencies;<sup>121</sup>
- taxation information—information provided by a taxpayer to a person or an agency pursuant to a legislative requirement contained in taxation legislation;<sup>122</sup>
- census and statistical information—information collected and maintained by the ABS under the *Census and Statistics Act 1905* (Cth);<sup>123</sup>
- electoral information—information collected and maintained by the Australian Electoral Commission under the *Commonwealth Electoral Act 1918* (Cth).<sup>124</sup>

10.109 In IP 34, the ALRC asked whether secrecy provisions should aim to protect specific types of information and, if so, what types of information should be protected by the provisions.<sup>125</sup>

### Submissions and consultations

10.110 In response, the AGD submitted that:

There may be specific types of information that, by their very nature, could cause harm and it is in the public interest that these types of information be protected from unauthorised disclosure. For example, the disclosure of Cabinet documents, regardless of the information contained in them, has the potential to prejudice the effective working of government by diminishing the government's faith that the Cabinet process provides a forum for free and frank debate and consideration of issues. Similarly, the disclosure of information provided to government by individuals and other non-government entities has the potential to harm public confidence in the government's ability to keep such information in confidence and only use it for the purpose for which it was provided.<sup>126</sup>

120 For example, *Defence Act 1903* (Cth) s 73A; *Defence Force Discipline Act 1982* (Cth) s 58; *Designs Act 2003* (Cth) s 108; *Criminal Code* (Cth) s 91.1.

121 For example, *Australian Federal Police Act 1979* (Cth) s 40ZA; *Australian Crime Commission Act 2002* (Cth) s 29B; *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 92.

122 See, eg, *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 55; *Child Support (Assessment) Act 1989* (Cth) s 150(2); *Inspector-General of Taxation Act 2003* (Cth) s 37(2).

123 *Census and Statistics Act 1905* (Cth) ss 19, 19A.

124 *Commonwealth Electoral Act 1918* (Cth) ss 90B, 91B, 189B, 323.

125 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 2–5.

126 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

10.111 A range of stakeholders commented on the information protected by secrecy offences relevant to their activities. For example, APRA stated that the definitions of ‘protected information’ and ‘protected documents’ in the APRA Act<sup>127</sup>

effectively capture information which should be protected (eg commercial in confidence information) while at the same time excluding information which should not be afforded protection (eg publicly available information).<sup>128</sup>

10.112 Similarly, other agencies highlighted the need to protect information such as: information that ‘could have a negative commercial impact on commercial entities’,<sup>129</sup> law enforcement-related information,<sup>130</sup> ‘personal and commercially sensitive information and financial transaction data’,<sup>131</sup> national security classified information;<sup>132</sup> and census and statistical information.<sup>133</sup>

10.113 DEEWR considered there to be merit in ‘greater scrutiny of the type of information which needs to be protected under agency legislation and supports the proposition that not all information held by an agency warrants additional protections in the form of secrecy or confidentiality provisions’.<sup>134</sup> Similarly, the DHS stated that the breadth of some secrecy provisions may give rise to unintended consequences.

For example, under the Centrelink provisions a registered business name containing the name of a customer (as a fictitious example, ‘Peter Piper Child Minding Pty Ltd’) would seem to come within the definition of protected information although it is unlikely that this was intended. Similarly, information about employees and contractors may fall within the same definitions if read literally. If it were a prerequisite to the application of a secrecy law that the information (both personal and non-personal) is inherently confidential in character, this would seem to overcome much of the problem. Dealings with non-confidential personal information would still be regulated by the *Privacy Act*.<sup>135</sup>

### **ALRC’s views**

10.114 In practice, the information protected by specific secrecy offences that apply to Commonwealth officers is usually a subset of the information that would be covered by the proposed new general secrecy offence. The general offence applies to all information to which a Commonwealth officer has, or had, access to by reason of being a Commonwealth officer.

---

127 Australian Prudential Regulation Authority Act 1998 (Cth) s 56(1).

128 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

129 Department of Climate Change, *Submission SR 27*, 23 February 2009.

130 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

131 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

132 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

133 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

134 Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

135 Department of Human Services, *Submission SR 26*, 20 February 2009.

10.115 Most existing specific secrecy offences apply to a subset of this information (such as personal information or confidential commercial information) acquired in the course of the officer's duties.<sup>136</sup> In other cases, the information protected by specific secrecy offences that apply to Commonwealth officers is effectively the same in scope—for example, where the offence applies to 'any information acquired' by a Commonwealth officer 'by reason of his or her office or employment under or for the purposes of this Act'.<sup>137</sup>

10.116 The reason the information protected by the proposed general secrecy offence is framed broadly is that the offence also requires that the nature of the information is such that its disclosure is reasonably likely to cause harm to specific public interests. Arguably, the information protected by a specific secrecy offence may, in practice, be adequately protected by the new general offence.

10.117 For example, many specific secrecy offences apply to the unauthorised disclosure of personal information or confidential commercial information held by Commonwealth officers.<sup>138</sup> The general secrecy offence applies where disclosure of the same information would have a substantial adverse effect on personal privacy or business, professional, commercial or financial affairs.

**Proposal 10–8** Specific secrecy offences that apply to Commonwealth officers should generally apply to all information to which a Commonwealth officer has, or had, access by reason of being a Commonwealth officer.

136 For example, *Higher Education Support Act 2003* (Cth) s 179-10; *Pooled Development Funds Act 1992* (Cth) s 76(5).

137 For example, under the *Australian Security Intelligence Organisation Act 1979* (Cth) s 81(1)(a).

138 See, eg, *Dental Benefits Act 2008* (Cth) s 34 (definition of 'entrusted public official').



# 11. Specific Secrecy Offences: Exceptions and Penalties

---

## Contents

Introduction	373
Exceptions and defences	373
Exceptions versus defences	374
Codification of permissible disclosure	376
Public interest disclosure	382
Consistency of exceptions	385
Penalties	389
Key principles	390
Appropriateness of criminal penalties	394
Consistency of penalties	395
Penalties and the <i>Crimes Act</i> provisions	396
Offences protecting similar information	398
Level of maximum penalty	404
Penalty benchmarks	405
Comparing penalties	405
Role of judicial discretion	406
Short sentences of imprisonment	407
Submissions and consultations	408
ALRC's views	409

## Introduction

11.1 This chapter discusses how specific secrecy offences should be framed in order to be more consistent with the proposed new general secrecy offence, and with each other, and highlights aspects of the general secrecy offence that might usefully be more broadly adopted. The key elements of the offences considered in this chapter are exceptions and defences, and penalties.

## Exceptions and defences

11.2 The proposed general secrecy offence would be subject to exceptions, where the disclosure is:

- in the course of a Commonwealth officer's functions or duties;

- authorised by the relevant agency head or minister, and the agency head or minister certifies that the disclosure is in the public interest; or
- of information that is already in the public domain as the result of a lawful disclosure.

11.3 Most Commonwealth secrecy provisions contain express exceptions or defences relating to the prohibited handling of information. These are summarised in Chapter 5 and include, for example, exceptions allowing information handling in the performance of a person's functions and duties as an employee or officer; and as required or authorised by law.

11.4 Individual secrecy offences often contain a number of different exceptions; and exceptions in each category are framed in many different ways. The exceptions contained in the proposed general secrecy offence are also commonly incorporated into specific secrecy offences, in one form or another. For example, the most common exceptions in specific secrecy offences are those that permit disclosure in the performance of a person's functions and duties; or as required or authorised by law. Exceptions that fall into one or both of these categories are present in approximately 65% of secrecy offences. In addition, about 20% of offences permit disclosure with the authority of the head of an agency or some other specified person, such as a minister.

11.5 Other common exceptions contained in specific secrecy offences are those that authorise disclosure to specified persons or entities, such as another Commonwealth agency (present in more than 35% of offences); and permit disclosure for the purposes of legal proceedings (20%), or for law enforcement (20%).

### **Exceptions versus defences**

11.6 A distinction may be made between exceptions and defences to Commonwealth secrecy offences. As noted in Chapter 9, an 'exception' is a provision that limits the scope of conduct prohibited by a secrecy offence; a 'defence' is a provision that may be relied on by a person whose conduct is prohibited by a secrecy offence.

11.7 In some respects, the distinction between an exception and a defence may be of limited significance. In raising either, the defendant faces an evidential burden. At common law, a defence is raised where, in the opinion of the trial judge, sufficient evidence is before the court to make it a genuine issue. In this sense, an evidential burden is placed upon a defendant to raise a defence.<sup>1</sup> The *Criminal Code* (Cth) provides that a defendant who 'wishes to rely on any exception, exemption, excuse, qualification or justification provided by the law creating an offence bears an evidential

---

<sup>1</sup> Thomson Legal and Regulatory, *The Laws of Australia*, Evidence, [16.3.4].

burden in relation to that matter'.<sup>2</sup> The prosecution must prove all the elements of an offence, positive and negative, and must also disprove any defences raised.<sup>3</sup>

11.8 While framing a provision as a defence, rather than as an exception, does not alter evidential or legal burdens of proof, it may have procedural disadvantages for a defendant. That is, a defendant will be forced to wait until the defence case is called before being able to lead evidence justifying a disclosure that would otherwise breach a secrecy provision.

#### **Submissions and consultations**

11.9 In the Issues Paper *Review of Secrecy Laws* (IP 34), the ALRC asked whether provisions in Commonwealth secrecy laws permitting the handling of information should generally be framed as exceptions or defences.<sup>4</sup>

11.10 The Law Council of Australia stated that, where relevant, there should only be exceptions rather than defences to secrecy offences for two main reasons:

- (a) The levelling of a charge tends to stigmatise notwithstanding the existence of an ultimately proven complete defence.
- (b) There are procedural disadvantages for a defendant in claiming a defence rather than being able to claim an exception.<sup>5</sup>

#### **ALRC's views**

11.11 In practice, while exceptions are commonly included in Commonwealth secrecy laws, only a few secrecy offences expressly provide defences.<sup>6</sup>

11.12 As discussed in Chapter 9, the Australian Government Attorney-General's Department (AGD) *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers (Guide to Framing Commonwealth Offences)* states that

a matter should be included in a defence, thereby placing the onus on the defendant, only where the matter is peculiarly within the knowledge of the defendant; and is significantly more difficult and costly for the prosecution to disprove than for the defendant to establish.<sup>7</sup>

2      *Criminal Code* (Cth) s 13.3(3). The Code states that the 'exception, exemption, excuse, qualification or justification need not accompany the description of the offence'. Notes in some Commonwealth secrecy laws refer to this provision of the *Criminal Code*: see, eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 65; *Taxation Administration Act 1953* (Cth) s 3(2A).

3      Thomson Legal and Regulatory, *The Laws of Australia*, Evidence, [16.3.4].

4      Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 4–3.

5      Law Council of Australia, *Submission SR 30*, 27 February 2009.

6      For example, *Aboriginal and Torres Strait Islander Act 2005* (Cth) ss 191(2A), 200A(3).

7      Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 28–29.

11.13 Defences may be available by virtue of the operation of the *Criminal Code*, which contains a number of defences of general application to Commonwealth offences. These include the defences of mistake or ignorance of fact, duress and lawful authority.<sup>8</sup> The AGD observed that these provisions:

are intended to codify the general defences available at common law. While specific defences are not excluded by the Code, careful consideration should be given to whether a proposed defence is already adequately covered by the general defences in the Code.<sup>9</sup>

11.14 In the ALRC's view, in the interests of consistency, specific secrecy offences that include defences should be reviewed to assess whether these defences are appropriate, in view of the general principles of criminal responsibility set out in ch 2 of the *Criminal Code*.

11.15 Where a defence is found to be appropriate, consideration should be given to recasting the provision as an exception, rather than as a defence. Rather than attempting to protect legitimate disclosure through a 'defence' that arises after a person has been found to satisfy all the elements of the offence, the ALRC considers that it would be better to frame secrecy offences in such a way that they do not extend to legitimate activities in the first place.<sup>10</sup>

**Proposal 11–1** Specific secrecy offences that include defences should be reviewed to assess whether these defences are appropriate, in view of the general principles of criminal responsibility set out in ch 2 of the *Criminal Code*. Where such a defence is found to be appropriate, consideration should be given to recasting the provision as an exception, rather than as a defence.

### Codification of permissible disclosure

11.16 While many secrecy laws contain identical or similar exceptions and defences—for example, providing that disclosure of information is not an offence when done in the performance of a person's duties—some provide detailed exceptions that permit disclosure for specified purposes or to specified persons or organisations.

11.17 A common formulation is to place a general prohibition on disclosure of certain information and to codify circumstances in which disclosure is allowed. Some of these provisions are extensive. The *Law Enforcement Integrity Commissioner Act 2006* (Cth), for example, contains exceptions to secrecy obligations placed on staff members

<sup>8</sup> *Criminal Code* (Cth) ss 9.1, 10.2, 10.5.

<sup>9</sup> Attorney-General's Department, *Submission SR 36*, 6 March 2009.

<sup>10</sup> A similar conclusion was reached in relation to the framing of sedition offences in Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), [12.70].

of the Australian Commission for Law Enforcement Integrity (ACLEI) allowing the Integrity Commissioner to disclose information to the heads of a range of specified Commonwealth, state and territory agencies.<sup>11</sup> Many other secrecy offences follow a similar approach.<sup>12</sup>

11.18 For example, the *Aged Care Act 1997* (Cth) provides a general prohibition on the disclosure of protected information by any person, subject to a limited number of exceptions, including where disclosure is in the performance of a function or duty under the Act.<sup>13</sup> In addition, the Secretary may disclose protected information in at least 12 separately defined circumstances,<sup>14</sup> such as ‘if a person has temporarily taken over the provision of care through a particular service to care recipients—to the person for the purposes of enabling the person properly to provide that care’.<sup>15</sup>

11.19 Many of these exceptions closely follow the wording of the Information Privacy Principles (IPPs) in the *Privacy Act 1988* (Cth), which set out limits on the use and disclosure of personal information held by agencies.<sup>16</sup> For example, in the *Aged Care Act*, the circumstances specified include where the Secretary

believes, on reasonable grounds, that disclosure of the information is reasonably necessary for: enforcement of the criminal law; or enforcement of a law imposing a pecuniary penalty; or protection of the public revenue; to an agency whose functions include that enforcement or protection, for the purposes of that enforcement or protection.<sup>17</sup>

11.20 Similarly, s 16 of the *Customs Administration Act 1985* (Cth) restricts the handling of information ('protected information')<sup>18</sup> unless certain exceptions apply.<sup>19</sup> Basic exceptions include disclosure as required or authorised by any other law; or in the course of performing the person's duties.

---

11       *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 208(3).

12       See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30; *Aged Care Act 1997* (Cth) ss 86-2, 86-3; *Dental Benefits Act 2008* (Cth) ss 34–41.

13       *Aged Care Act 1997* (Cth) s 86-2.

14       *Ibid* s 86-3.

15       *Ibid* s 86-3(g). The Secretary of the Department may also, for example, disclose protected information: where it is necessary in the public interest to do so; to a person who is expressly or impliedly authorised by the person to whom the information relates to obtain it; to the Chief Executive Officers of Medicare Australia and Centrelink, the Secretaries of Departments administering social security and veterans' entitlements, or to a state or territory for certain purposes; to prevent or lessen a serious risk to the safety, health or well-being of an aged care recipient; to a body responsible for standards of professional conduct; or for enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty, or protection of the public revenue; *Aged Care Act 1997* (Cth) s 86-3.

16       *Privacy Act 1988* (Cth) s 14, IPPs 10, 11.

17       *Aged Care Act 1997* (Cth) s 86-3(h).

18       ‘Protected information’ is defined as ‘information that directly or indirectly comes to the knowledge of, or into the possession of, a person while he or she is performing his or her duties’: *Customs Administration Act 1985* (Cth) s 16(1A).

19       *Ibid* ss 16(2)(c)–(e), 16(3), 16(3A)–(3H) sets out these exceptions.

11.21 In addition, if the ‘protected information’ also contains personal information, it cannot be disclosed without the consent of the person to whom the information relates, or unless the disclosure is made for a permissible purpose set out and the Chief Executive Officer (CEO) of the Australian Customs Service is satisfied that the disclosure is necessary for such a purpose.<sup>20</sup> Again, these permissible purposes have many similarities to use and disclosure that would be permitted under the *Privacy Act*.<sup>21</sup>

11.22 In relation to provisions containing extensive codification of the circumstances in which disclosure is allowed, John McGinness stated that:

any attempt to include such a code leads to further complexity in a secrecy provision and results in regular demands for amendment to deal with changing criteria for information sharing within government.<sup>22</sup>

11.23 The extensive codification of permissible disclosure needs to be considered in the context of demands for the effective sharing of Commonwealth information, including to support ‘whole of government’ responses to policy and administrative challenges.<sup>23</sup>

### ***Submissions and consultations***

11.24 In IP 34, the ALRC asked a number of questions relating to exceptions and defences to secrecy laws. In particular, the ALRC asked whether secrecy provisions should establish a general prohibition on disclosure and then attempt to codify, as in the examples discussed above, the circumstances in which disclosure is allowed.<sup>24</sup>

11.25 The AGD stated that codifying the circumstances in which disclosure is permitted ‘provides clarity and certainty to officers’ and may ensure that information collected by government agencies ‘is only used for the purpose it is collected or other limited appropriate purposes’.<sup>25</sup> Similarly, the Australian Intelligence Community (AIC) considered that ‘codification of the circumstances in which disclosure is allowed minimises the possible loopholes through which secret information may be publicly disclosed’.<sup>26</sup>

---

20 Ibid s 16(8).

21 See *Privacy Act 1988* (Cth) s 14, IPPs 10, 11; sch 3, NPP 2.

22 J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 62.

23 See Ch 3.

24 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 2–6.

25 Attorney-General’s Department, *Submission SR 36*, 6 March 2009. The AGD also expressed reservations about the potential inflexibility of this approach.

26 Australian Intelligence Community, *Submission SR 37*, 6 March 2009. The AIC noted that this is the current approach under the *Intelligence Services Act 2001* (Cth) ss 39, 39A, 40.

11.26 A number of other Australian Government agency stakeholders highlighted the advantages of such an approach to framing secrecy provisions.<sup>27</sup> The Australian Prudential Regulation Authority (APRA) observed, for example, that the approach in the *Australian Prudential Regulation Authority Act 1998* (Cth) (APRA Act) has ‘worked well’. APRA stated that:

If the secrecy provision is designed to protect information generated by government (augmenting the employee’s duty of fidelity), then it may need to be drafted using general language.

If, as with s 56 of the APRA Act, it is designed to protect information provided to government by third parties (either voluntarily in confidence or under compulsion), then it can and should be drafted in more specific terms, especially having regard to the need to provide clear exceptions.<sup>28</sup>

11.27 Some stakeholders referred to the decision of the High Court in *Johns v Australian Securities Commission (Johns)*<sup>29</sup> as one of the reasons secrecy offences need to be associated with comprehensive statutory exceptions.<sup>30</sup> In *Johns*, the High Court confirmed that a statute which confers a power to obtain information for a particular purpose limits, expressly or impliedly, the purposes for which the information obtained can then be used or disclosed. An agency that obtains information in the exercise of such a power is subject to a statutory duty of confidentiality. The information may not be used or disclosed except as authorised by the statute.<sup>31</sup>

11.28 The Treasury identified the limitations imposed by *Johns* on ‘the capacity of regulators to share certain information absent a legislative basis authorising disclosure’ as one reason for the enactment of comprehensive exceptions to the prohibition on disclosure of information set out in s 155AAA of the *Trade Practices Act 1974* (Cth).<sup>32</sup>

11.29 On the other hand, some stakeholders noted the possible inflexibility of codifying statutory exceptions to secrecy offences.<sup>33</sup> Ron Fraser observed that lengthy

27 For example, Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009; Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

28 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

29 *Johns v Australian Securities Commission* (1993) 178 CLR 408.

30 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; The Treasury, *Submission SR 22*, 19 February 2009.

31 *Johns v Australian Securities Commission* (1993) 178 CLR 408, 424 (Brennan J).

32 *Trade Practices Act 1974* (Cth) s 155AAA does not itself directly create a criminal offence. Breach of the secrecy obligations set out in s 155AAA may, however, found an offence under *Crimes Act 1914* (Cth) s 70.

33 R Fraser, *Submission SR 42*, 23 March 2009; Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

lists of exceptions, while often designed to facilitate the disclosure of information to other public authorities,<sup>34</sup> may create problems in practice.

There is often a need to add to these [exceptions and related guidelines], or amend them, to enable the agency to do its job properly eg, provision of information to another Commonwealth or State agency that is not specified in the exceptions, or return of innocuous information to providers of it where this is not specified. The fact that exceptions to the secrecy prohibitions occur in primary legislation makes this difficult to achieve quickly. It is, however, highly desirable for transparency reasons that provisions imposing criminal penalties, and the exceptions from them, appear in primary legislation. This is an example of the inflexibility and contradictions inherent in the classic secrecy provision.<sup>35</sup>

11.30 The tension in this area ‘between flexibility and accountability’ was also highlighted by the Department of Human Services (DHS). The DHS stated:

The more prescriptive the secrecy provision, the less able it is to deal with changes to methods and extent of service delivery. Whilst this may be a deliberate legislative decision, it creates service delivery frustrations which may be difficult to justify in practice to all those concerned including customers ... At the same time, if secrecy provisions are to instil a level of public comfort that information is being handled properly, there needs to be accountability and scrutiny beyond the limited interests of the agency which has possession of the information.<sup>36</sup>

11.31 Some stakeholders identified alternatives to prescriptive statutory provisions, such as authorisation by the minister or agency head. The DHS noted that ministerial determinations allowing disclosure in the public interest offer ‘the capacity to respond to changes more quickly than amendment to primary legislation, whilst retaining a level of parliamentary oversight’.<sup>37</sup> For example, the disclosure of social security information by Centrelink is permitted where the Secretary ‘certifies that it is necessary in the public interest to do so in a particular case or class of cases’. The issuing of such certificates is subject to Ministerial guidelines which are set out in a disallowable instrument.<sup>38</sup>

11.32 Other mechanisms include disclosure pursuant to memorandums of understanding and internal guidelines. The AGD submitted that:

Including a provision to enable the agency head or other senior officers to authorise disclosure may provide greater flexibility as it may enable disclosure in new or unforeseen circumstances. It also provides a level of accountability by requiring a senior officer to consider whether disclosure would be consistent with policy considerations in a particular case. Memorandums of understanding (MOU) or internal guidelines may also be used to set out circumstances when information can be disclosed from one agency to another. This may provide a more flexible approach, as

---

34 For example, *Health Insurance Act 1973* (Cth) s 130.

35 R Fraser, *Submission SR 42*, 23 March 2009.

36 Department of Human Services, *Submission SR 26*, 20 February 2009.

37 Ibid.

38 See *Social Security (Administration) Act 1999* (Cth) ss 208, 209.

the detail of information sharing arrangements can be left to documents more easily amended.<sup>39</sup>

#### **ALRC's views**

11.33 A major rationale for many exceptions contained in secrecy offences appears to be to clarify what kinds of use and disclosure are part of the functions of the agency, or are required or authorised by or under law, for the purposes of the agency complying with the *Privacy Act*.

11.34 The purpose of some exceptions is to protect privacy by detailing when disclosure is authorised. The Australian Transaction Reports and Analysis Centre (AUSTRAC) noted, for example, that the provisions of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) that comprehensively define authorised dealing with AUSTRAC information, were the result of privacy concerns:

AUSTRAC notes that various privacy and civil liberties organisations, including the Commonwealth Privacy Commissioner, participated in the development of the AML/CTF Act. There was a high level of support for stringent secrecy provisions, given the nature of AUSTRAC information.<sup>40</sup>

11.35 It is not clear that expressing such provisions as exceptions to a secrecy offence is a necessary or desirable approach. Secrecy provisions could be much simplified by relying on more generic exceptions that refer, for example, to disclosure in the performance of a function or duty under the Act or as required or authorised by law. Where extensive provisions authorising specific disclosure are required, these can be retained, even if associated specific secrecy offences are removed.

11.36 In the ALRC's view, specific secrecy offences that include extensive codification of permissible disclosure should be reviewed to establish whether these exceptions are necessary in view of the desirability of simplifying secrecy offences.

**Proposal 11–2** Specific secrecy offences that include extensive codification of permissible disclosure should be reviewed to establish whether these exceptions are necessary in view of the desirability of simplifying secrecy offences.

39 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

40 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

### **Public interest disclosure**

11.37 Another issue raised in submissions concerned the relationship between public interest disclosure, under proposed new Commonwealth public interest disclosure legislation, and exceptions or defences to specific secrecy offences.

11.38 As discussed in more detail in Chapter 9, the House of Representatives Standing Committee on Legal and Constitutional Affairs (the Standing Committee) has recommended that the Australian Government introduce legislation, entitled the Public Interest Disclosure Bill, to provide ‘whistleblower’ protections in the Australian Government public sector.<sup>41</sup>

11.39 The details of the proposed public interest disclosure legislation are set out in Chapter 9. In summary, the Standing Committee recommended that a broad range of Australian Government officials<sup>42</sup> be able to make public interest disclosures about ‘serious matters’<sup>43</sup> to their agency, or to designated external authorities such as the Commonwealth Ombudsman. A person who makes a public interest disclosure in accordance with the legislation would receive protections including immunity from: criminal liability (including under secrecy offences); liability for civil penalties and civil actions; and administrative sanctions.<sup>44</sup>

11.40 In addition, the Standing Committee recommended that protection extend to a person who makes a disclosure to the media

where the matter has been disclosed internally and externally, and has not been acted on in a reasonable time having regard to the nature of the matter, and the matter threatens immediate serious harm to public health and safety.<sup>45</sup>

11.41 The Standing Committee did not agree with suggestions that there be a blanket exclusion for security matters from public interest disclosure legislation or that the AIC agencies should be exempt from broader public interest disclosure procedures.<sup>46</sup> It recommended that where ‘disclosable conduct concerns a Commonwealth security or intelligence service, the authorised authorities to receive disclosures are the Inspector-General of Intelligence and Security and the Commonwealth Ombudsman’.<sup>47</sup>

11.42 In IP 34, the ALRC asked about the relationship between exceptions and defences provided under Commonwealth secrecy laws and possible new Commonwealth public interest disclosure legislation and, specifically, whether public

41 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 1.

42 Ibid, Rec 3.

43 Ibid, Rec 7.

44 Ibid, Rec 14.

45 Ibid, Rec 21.

46 Ibid, 129–130.

47 Ibid, Rec 19.

interest disclosure should be incorporated as an exception to criminal offences for unauthorised handling of Commonwealth information.<sup>48</sup> Such an exception might apply to any ‘public interest disclosure’ or ‘protected disclosure’, as defined in new public interest disclosure legislation, or to disclosure that fits some similar formulation.

11.43 The ALRC also asked whether new public interest disclosure legislation, if enacted, should exclude disclosure by Commonwealth officers employed by certain agencies—such as those involved in protecting national security.<sup>49</sup>

#### **Submissions and consultations**

11.44 As discussed in Chapter 9, a number of stakeholders supported incorporating public interest disclosure as an exception to secrecy offences. The New South Wales Young Lawyers Human Rights Committee, for example, submitted that ‘adequate protection must be extended to whistle blowing activities in the form of public interest exceptions to secrecy laws’.<sup>50</sup> The Commonwealth Ombudsman also supported protection against prosecution for breach of a secrecy provision for public interest disclosures.<sup>51</sup> The Community and Public Sector Union suggested that exceptions or defences to secrecy provisions should include disclosure where there is ‘suspicion of corrupt or illegal behaviour, national security [concerns] or where there is a clear public interest in disclosure’.<sup>52</sup>

11.45 In contrast, a number of agencies argued against a public interest disclosure exception relating to their relevant secrecy offences. For example, APRA stated that it would oppose the inclusion of a public interest disclosure exception in s 56 of the APRA Act, because ‘uncertainty’ about whether the exception would apply ‘may undermine the confidence of regulated entities, particularly regulated entities in financial difficulty, from being completely frank with APRA’.<sup>53</sup>

11.46 Similarly, the Australian Bureau of Statistics (ABS) stated that it did not believe that the disclosure of statistical information in breach of the *Census and Statistics Act 1905* (Cth) would ‘ever be in the public interest when balanced against the detriment to the public interest of the disclosure because of the weakening of official statistics’.

The ABS believes there are no circumstances that could justify circumvention of the *Census and Statistics Act 1905* secrecy provisions and no exceptions for ABS officers would be appropriate. It is highly unlikely that any benefits arising from a disclosure made in the public interest would outweigh the long-term damage to the ABS’s

---

48 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 4–6.

49 Ibid, Question 4–7.

50 NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009.

51 Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009.

52 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

53 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

reputation as a trusted data custodian, and consequently the quality of ABS statistics.<sup>54</sup>

11.47 The Australian Federal Police (AFP) was also ‘averse to the inclusion of public interest disclosure, or whistleblowing, exemptions within a proposed model secrecy offence framework’. Further:

Due to the nature of AFP operations, the associated requirement for complete integrity of our information holdings and our existing legislative framework for secrecy and protected disclosure the AFP would pursue exclusion of AFP employees from any general public interest disclosure legislation for the Australian Public Service or, at a minimum, restrict disclosures to an appropriate oversight agency such as the Commonwealth Law Enforcement Ombudsman or the Australian Commission for Law Enforcement Integrity.<sup>55</sup>

11.48 The AGD stated that secrecy laws ‘should not prevent people making lawful public interest disclosures in accordance with any established framework and legislation’, but suggested that in view of ‘the sensitivity of information held by security and intelligence agencies, it may be appropriate for there to be different procedures in place’, including a role for the Inspector-General of Intelligence and Security in receiving and investigating allegations in relation to security and intelligence agencies.<sup>56</sup>

#### *ALRC’s views*

11.49 As discussed in Chapter 9, the ALRC assumes, for the purpose of this Discussion Paper, that Commonwealth public interest disclosure legislation—based in large extent on the recommendations of the Standing Committee—will be enacted before the Australian Government considers the implementation of the ALRC’s final recommendations in this Inquiry.

11.50 The Standing Committee recommended that the protections provided under the public interest disclosure legislation should include immunity from criminal liability.<sup>57</sup> If so, there may be no useful purpose served by incorporating public interest disclosure exceptions into secrecy offences that apply in the same circumstances, as such exceptions would provide no additional protection.

11.51 In the ALRC’s view, however, it would be appropriate to include, in specific secrecy offence provisions that apply to Commonwealth officers, legislative notes referring to the fact that public interest disclosure legislation may provide immunity from criminal liability.

---

54 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

55 Australian Federal Police, *Submission SR 33*, 3 March 2009.

56 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

57 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 14.

11.52 The ALRC's final recommendations in this regard will depend, among other things, on how any new public interest disclosure legislation defines the categories of individual who can be protected, the types of disclosure that are protected, and the scope of the protection for individuals from administrative sanction and criminal and civil liability. As noted in Chapter 9, the ALRC may not have the benefit of considering the final form of public interest disclosure legislation before finalising its recommendations.

11.53 Chapter 9 discusses criticism of the scope of protection recommended by the Standing Committee for individuals making public interest disclosures to the media and other 'third parties'. The ALRC notes that, if the protection provided by public interest disclosure legislation is too limited, or the proposed legislation does not eventuate, it may be desirable to incorporate a public interest disclosure exception into the general secrecy offence.

11.54 The ALRC agrees with the conclusion of the Standing Committee that public interest disclosure legislation, if enacted, should not exclude disclosure by Commonwealth officers employed by certain agencies—such as those involved in protecting national security. This is consistent with recommendations made in previous ALRC reports. Notably, in *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), the ALRC recommended that the Commonwealth should legislate to introduce 'a comprehensive public interest disclosures scheme to cover all Australian Government agencies, including defence, security and intelligence agencies'.<sup>58</sup>

**Proposal 11–3** Specific secrecy offences that apply to Commonwealth officers should generally be accompanied by a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.

### Consistency of exceptions

11.55 In IP 34, the ALRC noted that the exceptions and defences provided by closely related secrecy legislation may vary significantly and it is not always clear that such variation is justifiable. Some of these apparent inconsistencies are discussed below.

58 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 3–1. The ALRC also recommended that this scheme should provide special procedures for dealing with disclosures from and about the defence, intelligence and security agencies and concerning classified and security sensitive information, including that disclosure should be made to the Inspector-General of Intelligence and Security in the first instance: Rec 3–2. See also: Australian Law Reform Commission, *Integrity: But Not by Trust Alone: AFP & NCA Complaints and Disciplinary Systems*, ALRC 82 (1996), Rec 117.

### ***Disclosure to ministers***

11.56 The Treasury's review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review) highlighted that these provisions can result in different degrees of disclosure to ministers according to the type of tax involved. In particular, information obtained for income tax purposes can be disclosed to a minister where it is in the performance of an officer's duties, but there is an absolute prohibition on the disclosure to ministers of information about indirect taxation, such as information relating to the GST.<sup>59</sup>

11.57 The exposure draft Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) (the Tax Laws Exposure Draft Bill) aims to remedy this by consolidating the relevant provisions in new sections of the *Taxation Administration Act 1953* (Cth), which would regulate disclosure to ministers and committees of Parliament and provide an exhaustive list of the circumstances where this can lawfully occur.<sup>60</sup>

11.58 Secrecy provisions applicable to the Australian Securities and Investments Commission (ASIC) and APRA, which operate under similar regulatory legislation, also take different approaches to disclosure to ministers. The *Australian Securities and Investments Commission Act 2001* (Cth) provides that disclosing information to the Minister amounts to 'authorised use and disclosure of the information'.<sup>61</sup> The APRA Act contains no similar exception to its secrecy provisions.

### ***Performance of duties***

11.59 Even where exceptions have a similar purpose, terminology is often inconsistent. The DHS highlighted this inconsistency of terminology:

In human services legislation the concept of 'performance of duties' is expressed in a variety of ways, including:

- 'in the performance of duties under or in relation to this Act' (*Child Support (Registration and Collection) Act* s 16);
- 'in the performance of duties, or in the exercise of powers or functions under this Act' (*National Health Act* s 135A); and
- 'authorised by or under the social security law' (ss 203 and 204 *Social Security (Administration) Act*).

---

59 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 21. See *Income Tax Assessment Act 1936* (Cth) s 16(2), (2A); cf *Taxation Administration Act 1953* (Cth) s 3C(2), (5)(a).

60 See Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.12]; Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 [355-55].

61 *Australian Securities and Investments Commission Act 2001* (Cth) s 127(2A).

This can be compared with other legislation eg s 16(2) *Income Tax Assessment Act 1936* which merely refers to ‘in performance of an officer’s duties’. Consistency of terminology would aid understanding.<sup>62</sup>

### **Disclosure with consent**

11.60 Another issue concerns the application of secrecy laws to the disclosure of personal information by Commonwealth officers with the consent of the person to whom the information relates. Some secrecy laws provide exceptions where the disclosure of personal information occurs with consent.<sup>63</sup> Other secrecy laws, such as those relating to officers of the Australian Taxation Office (ATO), do not permit such disclosure.<sup>64</sup>

11.61 The Treasury’s review of taxation secrecy and disclosure provisions noted that permitting the disclosure of information by the ATO with taxpayer consent would be in line with other secrecy laws.<sup>65</sup> The ATO itself observed that there would be ‘administrative benefits if a taxpayer could consent to his or her information being released to a third party’.<sup>66</sup>

11.62 The Treasury advised, however, that some organisations, responding to the review of taxation secrecy and disclosure provisions, expressed concern about such an approach because of the ‘inherent uncertainty’ about whether consent is informed and voluntary.<sup>67</sup> Under the Tax Laws Exposure Draft Bill, a taxpayer’s consent to the disclosure of information would not authorise the disclosure of that taxpayer’s information. The explanatory material to the Bill states:

This approach avoids issues of whether the consent is informed and voluntary (as opposed to, for instance, being a precondition for a particular good or service). This also recognises the fact that, if any entity requires the taxpayer’s information, the taxpayer is able to obtain that information and pass it on.<sup>68</sup>

### **Information in the public domain**

11.63 Some secrecy offences provide exceptions where information is already in the public domain.<sup>69</sup> Taxation secrecy laws, in contrast, may prevent the ATO from

---

62 Department of Human Services, *Submission SR 26*, 20 February 2009.

63 For example, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(4)(b); *Australian Federal Police Act 1979* (Cth) s 60A(2C).

64 *Income Tax Assessment Act 1936* (Cth) s 16.

65 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 27.

66 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

67 The Treasury, *Submission SR 22*, 19 February 2009.

68 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.15].

69 For example, *Criminal Code* (Cth) s 91.2; *Offshore Minerals Act 1994* (Cth) s 375. In some cases, the information protected by secrecy offences is defined to exclude information that has lawfully been made available to the public: eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(1) definitions of ‘protected document’ and ‘protected information’.

providing professional regulatory bodies with publicly available information, such as the fact that a barrister has been convicted of a taxation offence.<sup>70</sup>

11.64 The ATO suggested that there should be a provision stating that information already lawfully available to the public is not protected by tax secrecy provisions, including in order to investigate non-compliance with tax laws by ATO employees.<sup>71</sup> The Tax Laws Exposure Draft Bill provides that a taxation officer who discloses protected information does not commit an offence if the information was ‘already lawfully available to the public’.<sup>72</sup>

11.65 Other stakeholders also supported the application of exceptions relating to the disclosure of information that is in the public domain.<sup>73</sup> The Commonwealth Director of Public Prosecutions (CDPP), for example, stated that:

If investigation agencies are unable to publicise the outcomes of prosecutions the deterrent effect of successful prosecutions will be undermined. The CDPP also supports a defence or exception for the disclosure of de-identified information about a person/s.<sup>74</sup>

#### *ALRC’s views*

11.66 There is significant variation in the exceptions and defences that apply to specific secrecy offences. The great majority of these exceptions and defences are iterations of the exceptions provided for by the proposed general secrecy offence.<sup>75</sup> While consistency in exceptions, as between the general secrecy offence and specific secrecy offences, and between specific secrecy offences, is desirable, there are good reasons for many variations.

11.67 For example, the general secrecy offence would allow disclosure authorised by the relevant agency head or minister. The exception in the general secrecy offence is in such general terms because it must apply to many circumstances and provide sufficient flexibility to enable information flows.

11.68 While some secrecy offences contain a similar exception,<sup>76</sup> most that permit disclosure authorised by the agency head provide other criteria that must be met. Under the AML/CTF Act, for example, disclosure may be authorised by the CEO of

70 New South Wales Bar Association, *Submission to Treasury Review of Taxation Secrecy and Disclosure Provisions*, 26 September 2006.

71 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

72 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 [355-20]–[355-40].

73 Attorney-General’s Department, *Submission SR 36*, 6 March 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

74 Commonwealth Director of Public Prosecutions, *Submission SR 17*, 18 February 2009.

75 See Ch 9.

76 For example, *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C(5)(b).

AUSTRAC where the information will be used for investigating a breach of a law of the Commonwealth.<sup>77</sup>

11.69 The ATO emphasised that, in the context of taxation secrecy provisions, it would not be appropriate for disclosure to be made on the authority of a specified person (such as an agency head), because ‘this approach would provide less certainty for tax officers and taxpayers because of its discretionary nature’.<sup>78</sup>

11.70 In contrast, the *Income Tax Assessment Act 1936* (Cth) allows the Commissioner, a Second Commissioner, or a Deputy Commissioner of Taxation, or other persons authorised by those officers, to authorise disclosure to a wide range of specified bodies and purposes, set out in thirty separate subparagraphs.<sup>79</sup>

11.71 Similarly, while it may be appropriate for some specific secrecy offences to include an exception where disclosure is with the consent of the individual to whom the information relates, for the reasons discussed in Chapter 9 it would be inappropriate in the general secrecy offence.

11.72 Further, consent may not be an appropriate exception in the context of some specific secrecy offences. The option of a consent exception was rejected in the Tax Laws Exposure Draft Bill due to concerns about the validity of consent and a concern that the ATO is ‘not treated generally as a central repository of financial information to be accessed for purposes unrelated to the tax system or to government administration’.<sup>80</sup>

11.73 In the ALRC’s view, exceptions and defences applicable to specific secrecy offences should be reviewed for consistency with similar and related secrecy offences. However, exceptions to specific secrecy offences apply in a multitude of different circumstances and information-handling contexts. For this reason, this is not an area in which firm criteria against which to gauge consistency can be easily established, or where the general secrecy offence necessarily serves as a useful model.

## Penalties

11.74 As set out in Chapter 9, the ALRC proposes that the new general secrecy offence should have three tiers, with maximum penalties as follows:

---

<sup>77</sup> *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 129(1).

<sup>78</sup> Australian Taxation Office, *Submission SR 13*, 16 February 2009.

<sup>79</sup> *Income Tax Assessment Act 1936* (Cth) s 16(4)(a)–(m). The Tax Laws Amendment Exposure Draft Bill would, in the main, retain these provisions in a simplified form: See Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), 75, Table 8.4.

<sup>80</sup> Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.16].

- two years imprisonment for the first tier offence, where strict liability attaches to the requirement to prove harm;
- five years imprisonment for the second tier offence, where there is intention or recklessness as to the reasonable likelihood of harm to personal privacy or business, commercial or financial affairs; and
- seven years imprisonment for the third tier offence, where there is intention or recklessness as to the reasonable likelihood of harm to other specified public interests.<sup>81</sup>

11.75 As discussed in more detail below, the maximum penalties provided by specific secrecy offences vary widely, from a fine of \$110<sup>82</sup> to imprisonment for 25 years.<sup>83</sup> The following table provides a breakdown of the maximum penalties applicable to specific secrecy offences, by percentage of offences identified by the ALRC.<sup>84</sup>

<b>Penalty</b>	<b>%</b>
Pecuniary penalty only	10%
Imprisonment for 1 year or less	15%
Imprisonment for 2 years	66%
Imprisonment for 5 years	4%
Imprisonment for 7 years	1%
Imprisonment for 10 years	1%
Imprisonment for 15 years or more	1%

### **Key principles**

11.76 Before considering criminal penalties for specific secrecy offences, and how to achieve greater consistency in penalties, it is useful to examine briefly some principles and legislative provisions that apply in determining penalties for criminal offences generally.

---

81 Proposal 9–3.

82 *Reserve Bank Act 1959* (Cth) s 79B.

83 *Criminal Code* (Cth) s 91.1.

84 Percentages do not add up to 100 due to rounding to nearest percent.

### **Maximum penalties**

11.77 Provisions creating federal offences, including secrecy offences, typically specify the maximum penalty for the offence, which is intended for the worst type of case covered by the offence.<sup>85</sup> Parliament determines the maximum penalties, and courts in sentencing federal offenders are required to determine the sentence or order ‘that is of a severity appropriate in all the circumstances of the case’.<sup>86</sup>

11.78 The *Guide to Framing Commonwealth Offences*) states that ‘other than in rare cases, Commonwealth offences should carry a maximum penalty rather than a fixed penalty and should not carry a minimum penalty’.<sup>87</sup> Under s 4D of the *Crimes Act 1914* (Cth), the specified penalty for a Commonwealth offence is to be read as being a maximum only, unless the contrary intention appears.

### **Types of penalty**

11.79 The maximum penalty in provisions creating offences is normally expressed in terms of a monetary penalty, penalty units,<sup>88</sup> or a term of imprisonment. In the case of secrecy offences, in the majority of cases, the court has the option of imposing a fine,<sup>89</sup> a term of imprisonment or both. There are, however, some secrecy provisions that specify a fine only.<sup>90</sup>

11.80 Section 17A of the *Crimes Act* reflects the common law position that imprisonment is a sentencing option of last resort.<sup>91</sup> The section provides that a court is not to impose a sentence of imprisonment unless it is satisfied that no other sentence is appropriate in all the circumstances of the case.

11.81 Options apart from fines and imprisonment are available in sentencing federal offenders. Some of these options are expressly set out in Part IB of the *Crimes Act*.

---

85 *Ibbs v The Queen* (1987) 163 CLR 447, 451–452; *Veen v The Queen [No 2]* (1988) 164 CLR 465, 478.

86 *Crimes Act 1914* (Cth) s 16A(1).

87 Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 39. The ALRC has previously recommended that no mandatory minimum term of imprisonment should be prescribed for any federal offence: Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), Rec 21–3.

88 A penalty unit is defined in the *Crimes Act 1914* (Cth) s 4AA as \$110, unless the contrary intention appears.

89 As discussed below, if the offence provision does not specify a maximum fine, there is a formula for calculating the maximum fine that would apply.

90 For example, *Aboriginal and Torres Strait Islander Act 2005* (Cth) s191; *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63(2); *Child Support (Registration and Collection) Act 1988* (Cth) s 58; *Ombudsman Act 1976* (Cth) s 35(2); *Civil Aviation Regulations 1988* (Cth) reg 132(3).

91 See R Fox and A Freiberg, *Sentencing: State and Federal Law in Victoria* (1999), [9.205]. This approach was endorsed by the ALRC in Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), [7.145].

Others are picked up from state and territory law by the *Crimes Act* and regulations made under the Act.<sup>92</sup>

11.82 The *Crimes Act* contains a number of provisions relevant to determining the fine that can be imposed on a natural person or corporation for breaching a federal secrecy provision.

#### ***Penalty conversions where only imprisonment is specified***

11.83 Where an offence provision refers only to imprisonment, s 4B(2) and (2A) of the *Crimes Act* enable a court to impose a fine if it considers it appropriate to do so. Section 4B(2) sets out a formula to determine the amount of penalty units, being:

Term of Imprisonment x 5

where:

**Term of Imprisonment** is the maximum term of imprisonment, expressed in months, by which the offence is punishable.

11.84 Section 4B(2) of the *Crimes Act* plays a key role in determining the maximum fines that can be imposed for breaches of federal secrecy provisions as a significant number of such provisions are expressed to be punishable by imprisonment only.<sup>93</sup> For example, if a provision specifies a term of imprisonment of two years, the applicable fine is 120 penalty units ( $24 \times 5$ )—amounting to \$13,200 ( $120 \times \$110$ ). Fines referred to in this chapter have been calculated with reference to s 4B of the *Crimes Act*, where applicable.

11.85 Section 4B(2A) provides that if an offence provides for imprisonment for life, the court may impose a maximum pecuniary penalty of 2,000 penalty units.

#### ***Penalty conversion where fine expressed in monetary terms***

11.86 A number of secrecy offences specify a maximum fine in dollar terms rather than penalty units.<sup>94</sup> Section 4AB of the *Crimes Act* sets out a formula for converting monetary penalties expressed in dollar amounts to penalty units.<sup>95</sup> References to fines in this chapter take into account the application of s 4AB, where applicable.

#### ***Alternate penalties for proceeding summarily on an indictable offence***

11.87 Summary offences are those that are either not punishable by imprisonment, or are punishable by imprisonment for a period not exceeding 12 months, unless the

92 A detailed examination of sentencing options for federal offenders is discussed in Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), Ch 7.

93 Examples of such provisions are discussed below in the section on consistency of penalties.

94 For example, *Australian Institute of Health and Welfare Act 1987* (Cth) s 29 and *Australian Trade Commission Act 1985* (Cth) s 94 each provide for a maximum fine of \$2,000.

95 For example, if a secrecy provision specifies a fine of \$2,000, with the application of *Crimes Act 1914* (Cth) s 4AB, the fine is actually \$2,200.

contrary intention appears.<sup>96</sup> Indictable federal offences are those that are punishable by imprisonment for a period exceeding 12 months, unless the contrary intention appears.<sup>97</sup>

11.88 Some federal secrecy provisions specify alternate maximum penalties, depending on whether the offence is dealt with summarily (that is, without a jury) or on indictment.<sup>98</sup> The *Crimes Act* provides that certain indictable offences punishable by imprisonment for a period not exceeding 10 years may, unless the contrary intention appears, be dealt with summarily where both the prosecutor and the defendant consent.<sup>99</sup>

11.89 Where a federal secrecy offence is able to be dealt with summarily under the provisions of the *Crimes Act*, the following reduced penalties apply:

- in the case of offences punishable by imprisonment for a period not exceeding five years, the maximum penalty is reduced to a sentence of imprisonment for a period not exceeding 12 months or a fine not exceeding 60 penalty units or both; and
- in the case of offences punishable by imprisonment for a period greater than five years and less than 10 years, the maximum penalty is reduced to a sentence of imprisonment not exceeding two years or a fine not exceeding 120 penalty units or both.<sup>100</sup>

### ***Penalties for corporations***

11.90 Secrecy offence provisions typically specify the maximum fine or sentence of imprisonment that can be imposed on a natural person. They do not usually specify separate maximum penalties for corporations, although a few provisions do so.<sup>101</sup>

11.91 Many of the sentences that can be imposed on natural persons cannot be imposed on corporations—for example, a corporation cannot be sentenced to imprisonment.<sup>102</sup> Section 4B(3) of the *Crimes Act* empowers a court sentencing a corporation to impose a pecuniary penalty that is up to five times greater than the

---

96 Ibid s 4H.

97 Ibid s 4G.

98 Examples of such provisions are discussed below in the section on consistency of penalties.

99 *Crimes Act 1914* (Cth) s 4J. Some secrecy offences such as s 79(2), (5) of the *Crimes Act* cannot be dealt with summarily: s 4J(7).

100 Ibid s 4J.

101 For example, *Sex Discrimination Act 1984* (Cth) s 92; *Defence Act 1903* (Cth) s 73F.

102 The ALRC made a number of recommendations about sentencing options that should be available in sentencing corporations in Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), Ch 30.

maximum penalty that could be imposed on a natural person convicted of the same offence, provided that the contrary intention does not appear in the offence provision.

### **Appropriateness of criminal penalties**

11.92 In IP 34, the ALRC considered the circumstances in which it may be appropriate for criminal penalties to apply when a secrecy provision has been breached. A range of relevant factors have been identified by commentators, including: the nature of the information the subject of protection; the intent of the offender; the adverse consequences of a criminal conviction; the seriousness of the breach; and the effect on the public interest if the information were to be disclosed.<sup>103</sup>

11.93 The ALRC asked when unauthorised handling of Commonwealth information should be subject to criminal penalties; and which factors should determine whether or not it is appropriate for criminal penalties to apply.<sup>104</sup>

#### ***Submissions and consultations***

11.94 The AGD emphasised that a criminal offence is the ultimate sanction for breaching the law.

Criminal offences should be used where the relevant conduct involves considerable harm to society, the environment or Australia's national interests, including security interests. One important factor to consider when deciding whether a criminal offence is appropriate is the effect of a criminal offence. A criminal conviction carries with it a social stigma, particularly where the conviction is accompanied by imprisonment.<sup>105</sup>

11.95 Stakeholders referred to factors that need to be taken into account in determining whether criminal penalties are justified. The Treasury stated that these included the nature of the information protected, how it was obtained by the agency holding it and the potential impact of unauthorised release.<sup>106</sup>

11.96 The Public Interest Advocacy Centre (PIAC) expressed broad agreement that the factors identified in IP 34 should be taken into account in determining whether criminal penalties should apply. However, in PIAC's opinion,

Disclosure of information obtained in the course of official duties (apart from information relating to defence, security and law enforcement) should rarely, if ever, amount to a criminal offence, as opposed to attracting a civil penalty.<sup>107</sup>

11.97 Liberty Victoria agreed that criminal penalties should be applied if there is 'intent to mishandle information'. Penalties should be applied 'on a sliding scale of punishment applied by the courts based on a number of factors including the

---

103 See Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), [5.39]–[5.43].

104 Ibid, Question 5–1.

105 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

106 The Treasury, *Submission SR 22*, 19 February 2009.

107 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

classification of the information, and whether or not the conduct was intended to cause harm'.<sup>108</sup>

11.98 PIAC stated that 'intent at the level of carelessness' should not be enough to justify the imposition of criminal liability, except perhaps 'where very serious damage to life and limb has been the direct result'.<sup>109</sup> ASIC also focused on intention as the critical factor in determining whether criminal liability should apply, stating that there is a stronger argument for such penalties if the offender 'deliberately discloses information for profit or with malicious intent'.<sup>110</sup>

#### **ALRC's views**

11.99 Commonwealth information includes a range of highly sensitive information—for example, national security information, information relating to defence, valuable commercial information and sensitive personal information. The unauthorised disclosure of Commonwealth information has the capacity to cause real harm to important public interests. In the ALRC's view, criminal penalties are appropriate, at least where unauthorised disclosure is reasonably likely to cause such harm.

### **Consistency of penalties**

11.100 The Terms of Reference for this Inquiry require the ALRC to consider options for ensuring a consistent approach across government to the protection of Commonwealth information.<sup>111</sup> A significant aspect of this consistency of approach is consistency of penalties for secrecy offences.

11.101 The AGD *Guide to Framing Commonwealth Offences* directs those framing offences to 'ensure [the] penalty fits with other penalties in Commonwealth law'.<sup>112</sup>

Penalties should be framed to maximise consistency with penalties for existing offences of a similar kind or of similar seriousness. Penalties within a given legislative regime should reflect the relative seriousness of the offences within that scheme.<sup>113</sup>

11.102 The Senate Scrutiny of Bills Committee has stated that 'consistency is the main aim of criminal law policy when determining penalties'.<sup>114</sup> Similarly, the Standing Committee has expressed the view that 'consistency in the range and expression of penalties in criminal secrecy provisions is desirable,' although 'there

108 Liberty Victoria, *Submission SR 19*, 18 February 2009.

109 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

110 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

111 The Terms of Reference are set out at the front of this Discussion Paper.

112 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 38.

113 Ibid, 38.

114 Parliament of Australia Senate Scrutiny of Bills Committee, *Scrutiny of Bills Eighth Report of 1998* (1998), [3.8].

may need to be some flexibility depending on the sensitivity of the information to be protected'.<sup>115</sup>

11.103 More recently, the Taxation Secrecy Review recommended that penalties for unauthorised disclosure of protected information should be standardised.<sup>116</sup> This is reflected in the Tax Laws Exposure Draft Bill, which provides a standard penalty of imprisonment of up to two years and a fine of up to 120 penalty units (\$13,200).<sup>117</sup>

11.104 There are a number of different ways of examining the consistency of penalties provided in secrecy offences. Consistency can be assessed by comparing the penalties:

- in secrecy offence provisions to those which would otherwise apply if formulas in the *Crimes Act* were to apply; and
- between secrecy offence provisions that aim to protect similar types of information.

### **Penalties and the *Crimes Act* provisions**

11.105 In IP 34, the ALRC detailed a range of inconsistencies in penalties, identified on the basis of the above comparisons.<sup>118</sup> In relation to the provisions contained in the *Crimes Act*, these inconsistencies included that:

- the fine to imprisonment ratio provided by some secrecy offences differs—to varying degrees—from the standard ratio of five penalty units to one month of imprisonment (5:1 ratio) set out in s 4B of the *Crimes Act*;<sup>119</sup>
- the maximum fines applicable to bodies corporate provided under some secrecy offences differ from the ‘5 times’ multiplier provided by s 4B(3) of the *Crimes Act*;<sup>120</sup>

---

115 Australian Parliament—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), 96–97.

116 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), Principle 6.

117 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 ss 355-20, 355-155, 355-265.

118 See Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), [5.48]–[5.77].

119 For example, the ratio provided by the *Excise Act 1901* (Cth) s 159 is more than 20:1 (500 penalty units and 2 years imprisonment). Under the *Australian Institute of Health and Welfare Act 1987* (Cth) s 29, the ratio is less than 2:1 (20 penalty units and 1 years imprisonment). Drafting guidelines for Commonwealth offences instruct drafters to adopt the 5:1 ratio ‘unless there are grounds to depart from it’: Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 41.

120 For example, *Defence Act 1903* (Cth) s 73F(2) prescribes a maximum fine for a body corporate 10 times that which can be imposed on a natural person.

- some indictable secrecy offences provide for penalties where the offence is dealt with summarily that differ from those provided by s 4J(3) of the *Crimes Act*,<sup>121</sup> and
- some secrecy provisions specify a penalty punishable on summary conviction when, under s 4H of the *Crimes Act*, an offence carrying that maximum penalty would otherwise be tried before a jury on indictment.<sup>122</sup>

11.106 In IP 34, the ALRC asked questions about the circumstances in which such inconsistencies might be appropriate.<sup>123</sup> Stakeholders who commented on these issues submitted that secrecy offences should provide penalties that are consistent with the general provisions of Part IA of the *Crimes Act* and did not suggest any circumstances that might justify departure from them.<sup>124</sup> In the ALRC's view, there appears to be no justification for inconsistency between the penalties in specific secrecy offences and the approach prescribed by the *Crimes Act* and such inconsistency should be remedied.

**Proposal 11–4** In order to ensure consistency, secrecy offence provisions should not specify:

- (a) fines for individuals and corporations different from those that would apply if the formulas set out in the *Crimes Act 1914* (Cth) were adopted;
- (b) penalties different from those that would apply if the alternate penalties for proceeding summarily on an indictable offence set out in the *Crimes Act* were adopted; or
- (c) a penalty punishable on summary conviction when, under the *Crimes Act*, an offence carrying that maximum penalty would otherwise be tried before a jury on indictment.

121 For example, *Disability Services Act 1986* (Cth) s 28 and *Telecommunications (Interception and Access) Act 1979* (Cth) s 105 provide for a maximum term of six months imprisonment on a summary conviction, which is 50% less than would otherwise apply under *Crimes Act 1914* (Cth) s 4J.

122 For example, *Taxation (Interest on Overpayments and Early Payments) Act 1983* (Cth) s 8 provides for a maximum penalty of two years imprisonment and an \$11,000 fine, punishable on summary conviction.

123 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Questions 5–2, 5–3.

124 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; Attorney-General's Department, *Submission SR 36*, 6 March 2009; The Treasury, *Submission SR 22*, 19 February 2009.

## **Offences protecting similar information**

11.107 There is wide variation in the maximum penalties provided by secrecy offences protecting very similar types of information. Some of these variations are discussed below, with reference to:

- information relating to the affairs of a person;
- information obtained in the course of duties;
- information relating to law enforcement and investigations;
- defence or security information;
- confidential information;
- information the disclosure of which is expected to prejudice financial interests; and
- initial and subsequent disclosure of the same information.<sup>125</sup>

### ***Information relating to the affairs of a person***

11.108 Penalties for offences involving the unauthorised acquisition, recording or disclosure of information about the affairs of another person differ widely. A small number of these offences carry a maximum penalty of a fine only.<sup>126</sup> Most, however, are punishable either by a fine or a period of imprisonment, or both. The maximum term of imprisonment for such offences varies from three months<sup>127</sup> to two years,<sup>128</sup> with the majority carrying the latter penalty and, therefore, qualifying as indictable offences.

11.109 It is difficult to justify this level of inconsistency, which can be illustrated by comparing the penalties for the following two offences:

- The maximum penalty that applies to officers performing functions under the *Health Insurance Act 1973* (Cth) for the unauthorised disclosure of ‘information

---

125 A fuller discussion of this variation is set out in Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), [5.61]–[5.75].

126 For example, *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 191 (\$5,500); *Child Support (Registration and Collection) Act 1988* (Cth) s 58 (\$1,100); *Health Insurance Act 1973* (Cth) s 130(1) (\$550).

127 For example, *Port Statistics Act 1977* (Cth) s 7(1); *Social Welfare Commission (Repeal) Act 1976* (Cth) s 8(1).

128 For example, *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 55; *Aged Care Act 1997* (Cth) s 86-2; *Disability Discrimination Act 1992* (Cth) s 127; *Higher Education Funding Act 1988* (Cth) s 78(4); *Disability Services Act 1986* (Cth) ss 28(2), 29(1); *National Health Act 1953* (Cth) s 135A.

with respect to the affairs of another person'—including, for example, a person's Medicare records—is a fine of \$550.<sup>129</sup>

- The maximum penalty that applies to officers performing functions under the *National Health Act 1953* (Cth) for the unauthorised disclosure of similar information is \$5,500 or imprisonment for two years, or both.<sup>130</sup>

#### ***Information obtained in the course of official duties***

11.110 The penalties for breaching secrecy provisions that protect information acquired in the course of official duties also vary widely. At least one provision is punishable by a maximum penalty of a fine only, in the amount of \$550.<sup>131</sup> The majority, however, are punishable by a term of imprisonment and fine. The maximum term of imprisonment varies from six months<sup>132</sup> to two years,<sup>133</sup> with the majority carrying the latter term of imprisonment and a fine of \$13,200.

11.111 One significant example of inconsistency is the penalties that attach to provisions protecting information acquired in the course of performing law enforcement duties:<sup>134</sup>

- The maximum penalty that applies to members and staff of the Australian Crime Commission (ACC) for recording, divulging or communicating information acquired in the performance of their duties or functions is a term of imprisonment for one year and a \$5,500 fine;<sup>135</sup>
- The maximum penalty applying to members, employees and persons engaged by the AFP for engaging in similar conduct is two years imprisonment and a fine of \$13,200.<sup>136</sup>

11.112 It is not clear that there is any significant difference between the nature or sensitivity of the information handled by the ACC and the AFP that would justify this disparity.

---

129 *Health Insurance Act 1973* (Cth) s 130(1).

130 *National Health Act 1953* (Cth) s 135A.

131 *Ombudsman Act 1976* (Cth) s 35(2).

132 *Parliamentary Commission of Inquiry (Repeal) Act 1986* (Cth) s 7.

133 For example, *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34; *Customs Administration Act 1985* (Cth) s 16; *Australian Federal Police Act 1979* (Cth) s 60A; *Australian Security Intelligence Organisation Act 1979* (Cth) s 81; *Trade Practices Act 1974* (Cth) ss 95ZP, 95ZQ.

134 Penalties for breach of secrecy provisions protecting information relating to law enforcement and investigations are considered separately below.

135 *Australian Crime Commission Act 2002* (Cth) s 51.

136 *Australian Federal Police Act 1979* (Cth) s 60A.

### ***Information relating to law enforcement and investigations***

11.113 There are a variety of secrecy provisions that aim to protect the integrity of the investigation and law enforcement processes. The particular information which is targeted by these provisions varies in its specificity and scope, making it more difficult to draw general conclusions about consistency. Further, some provisions include as an element of the offence the effect of the disclosure of information of this type.<sup>137</sup> Some offences carry a maximum penalty of a fine only.<sup>138</sup> The maximum terms of imprisonment for offences in this category vary from one year<sup>139</sup> to 10 years.<sup>140</sup>

11.114 Some examples of penalties that seem inconsistent are found in provisions concerning investigation records:

- Under the *Space Activities Act 1998* (Cth), an investigation officer is subject to a maximum fine of \$3,300 if he or she discloses a ‘safety record’ in circumstances other than those set out in the provision. A ‘safety record’ includes all statements taken in the course of investigation of an accident, and all communications between persons involved in operating a space object that is involved in an accident.<sup>141</sup>
- Under the *Transport Safety Investigation Act 2003* (Cth), a person who is or has been a staff member is subject to a fine of \$13,200 and imprisonment for two years, if he or she discloses ‘restricted information’.<sup>142</sup> The definition of ‘restricted information’ is similar to the definition of ‘safety record’ in the *Space Activities Act*.<sup>143</sup>

### ***Defence or security information***

11.115 Not surprisingly, the highest maximum penalties for breach of secrecy provisions are found in provisions that protect defence or security information. The range of maximum penalties varies from imprisonment for ‘any term’ and a fine of ‘any amount’,<sup>144</sup> to imprisonment for six months and a fine of \$3,300.<sup>145</sup>

---

137 For example, *Witness Protection Act 1994* (Cth) s 22(1); *Surveillance Devices Act 2004* (Cth) s 45(2).

138 For example, *Space Activities Act 1998* (Cth) s 96; *Australian Federal Police Act 1979* (Cth) s 40ZA.

139 For example, *Australian Security Intelligence Organisation Act 1979* (Cth) s 92.

140 For example, *Surveillance Devices Act 2004* (Cth) s 45(2); *Witness Protection Act 1994* (Cth) s 22(1).

141 *Space Activities Act 1998* (Cth) s 96.

142 *Transport Safety Investigation Act 2003* (Cth) s 60.

143 It includes all statements obtained in the course of an investigation, and all communication with a person involved in the operation of a transport vehicle that is or was the subject of an investigation: *Ibid* s 3.

144 *Defence Act 1903* (Cth) ss 73A, 73F.

145 *Crimes Act 1914* (Cth) s 79(4).

11.116 The conduct prohibited by these provisions varies widely. Nevertheless, some disparities appear hard to justify. For example:

- the maximum penalty for espionage—where a person communicates information concerning the Commonwealth’s security or defence, intending to prejudice the Commonwealth’s security or defence, and the person’s act is likely to result in the information being communicated to another country or a foreign organisation—is imprisonment for 25 years;<sup>146</sup>
- the maximum penalty for a defence member or defence civilian who discloses information likely to be prejudicial to the security or defence of Australia without lawful authority is imprisonment for 2 years.<sup>147</sup>

#### ***Confidential information***

11.117 A number of secrecy provisions aim to protect information that is supplied in confidence, or is confidential in nature. Most such provisions are punishable on breach with a maximum penalty of two years imprisonment and a fine of \$13,200.<sup>148</sup>

11.118 In comparison, the maximum penalty for the unauthorised disclosure, production, recording or use of any confidential information acquired in the course of duties under the *Equal Opportunity for Women in the Workplace Act 1999* (Cth) is significantly less—imprisonment for three months and a fine of \$2,750.

#### ***Disclosure of information prejudicial to financial interests***

11.119 Under the *Aboriginal and Torres Strait Islander Act 2005* (Cth), an officer of an Indigenous Land Corporation is subject to a maximum term of imprisonment for one year and a \$6,600 fine if he or she discloses information that relates to the affairs of a person obtained in the course of duties where disclosure could reasonably be expected to substantially prejudice the person’s commercial interests.<sup>149</sup>

11.120 In contrast, under the *Pooled Development Funds Act 1992* (Cth), a person who discloses information ‘which may reasonably be expected to affect a person adversely in respect of the lawful business, commercial or financial affairs of the person’, is subject to double the above-mentioned maximum penalty—that is, two years imprisonment and a fine in the amount of \$13,200.<sup>150</sup>

---

146 *Criminal Code* (Cth) s 91.1(1).

147 *Defence Force Discipline Act 1982* (Cth) s 58.

148 For example, *Gene Technology Act 2000* (Cth) s 187; *Chemical Weapons (Prohibition) Act 1994* (Cth) s 102; *Pooled Development Funds Act 1992* (Cth) s 71.

149 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S.

150 *Pooled Development Funds Act 1992* (Cth) s 71.

### ***Initial and subsequent disclosure***

11.121 Many secrecy provisions apply only to the initial unauthorised handling of Commonwealth information.<sup>151</sup> This is typically an unauthorised disclosure by an officer of the relevant agency who possesses the protected information. Other secrecy provisions also seek to regulate the conduct of those persons who receive protected information pursuant to an initial disclosure—whether authorised or unauthorised.

11.122 Existing penalties for initial and subsequent disclosure of protected information are sometimes consistent, as in the AML/CTF Act<sup>152</sup> and the *Aged Care Act 1997*.<sup>153</sup>

11.123 In other cases, penalties differ. For example, under the *Health Insurance Act*, where protected information is disclosed to a person in contravention of s 130, the person is guilty of an offence if he or she discloses the information to another person where he or she knows, or reasonably ought to know, that the disclosure is in breach.<sup>154</sup> The maximum penalty for this subsequent disclosure is two years imprisonment.<sup>155</sup> An officer making the initial unauthorised disclosure is liable only to a fine of \$550.<sup>156</sup>

### ***Submissions and consultations***

11.124 Stakeholders highlighted lack of consistency in existing penalties for breach of secrecy provisions.<sup>157</sup> The DHS, for example, noted that penalties vary across its portfolio legislation.

For example, the penalty for an employee disclosing (however termed) protected information ranges from \$500 (*Health Insurance Act*) to 2 years imprisonment and 120 penalty units (\$13,200 at the time of writing) (*Dental Benefits Act*). Medicare Australia advises that the information protected under the *Health Insurance Act* and the *Dental Benefits Act* is essentially the same.<sup>158</sup>

11.125 The DHS stated that these anomalies are even more noticeable within agencies subjected to more than one secrecy provision. For example, a Medicare Australia employee who discloses information protected under the *National Health Act* faces a maximum fine ten times that of an officer committing the same offence under the *Health Insurance Act*, and only the former attracts a sentence of imprisonment.<sup>159</sup>

---

151 For example, *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).

152 See *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 121(2), (7), (12).

153 *Aged Care Act 1997* (Cth) ss 86-2, 86-5.

154 *Health Insurance Act 1973* (Cth) s 130(15).

155 *Ibid* s 130(23).

156 *Ibid* s 130(1).

157 For example, Law Council of Australia, *Submission SR 30*, 27 February 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

158 Department of Human Services, *Submission SR 26*, 20 February 2009.

159 *Ibid*.

Even within the same Act there are apparent inconsistencies. Under the *Health Insurance Act* a person who offers to supply protected information can be imprisoned for 2 years, whereas the maximum penalty for actually doing so is \$500. Under Centrelink's legislation, the Secretary can authorise disclosure in the public interest, but cannot authorise use on the same footing.<sup>160</sup>

11.126 ACLEI noted that inconsistent penalty provisions apply to employees of the ACC and the AFP, and submitted that the former should be made consistent with that which applies under the *Australian Federal Police Act 1979* (Cth).<sup>161</sup> The Law Council agreed that 'currently there is a high degree of inconsistency among the various pieces of legislation, without any apparent reason for the inconsistency'.<sup>162</sup>

11.127 In IP 34, the ALRC asked about the best way to achieve consistency in the maximum criminal penalties for breach of secrecy provisions, and what factors should be taken into account in arriving at penalties for secrecy offences—such as the type of information protected, conduct proscribed, the fault element, and whether or not the conduct harmed the public interest.<sup>163</sup>

11.128 The AGD stated that it is 'a well established legal principle that similar offences should have similar penalties'. The AGD noted that maximum penalties can be set by reference to the fault elements that apply, as well as to the potential harm that could be caused by the relevant conduct.<sup>164</sup>

11.129 The Law Council submitted that maximum penalties for secrecy offences should be 'identified and set by reference to the kind of information protected'.<sup>165</sup> ASIC agreed that the factors mentioned in IP 34 were relevant and also referred to the relevance of harm to 'private' interests, such as commercial interests. PIAC submitted that:

the preferred approach should be to seek consistency in maximum penalties based on the following factors: the nature and volume of the material in question; the nature and extent of any harm or potential harm to identified public interests; the intent and motive of the defendant; the level of seniority and office held by the defendant; and any countervailing public interest factors.<sup>166</sup>

11.130 The ALRC also asked whether penalties should be consistent for both the initial and subsequent unauthorised handling of Commonwealth information.<sup>167</sup> Most

160 Ibid.

161 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009, referring to *Australian Crime Commission Act 2002* (Cth) s 51; *Australian Federal Police Act 1979* (Cth) s 60A.

162 Law Council of Australia, *Submission SR 30*, 27 February 2009.

163 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–4.

164 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

165 Law Council of Australia, *Submission SR 30*, 27 February 2009.

166 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

167 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–5.

stakeholders who addressed the issue considered that penalties should generally be the same for both.<sup>168</sup> For example, as noted in Chapter 9, the AGD stated that

if the fault elements and harm caused by the conduct are the same, it would be reasonable for the penalty to be the same regardless of whether the offence is one of first or subsequent unauthorised handling.<sup>169</sup>

11.131 PIAC submitted the penalties for subsequent handling ‘should be of a lower order, except where intent to damage Australia’s national interest is proven’.<sup>170</sup>

#### *ALRC’s views*

11.132 There is wide variation in the maximum penalties provided by secrecy offences protecting very similar types of information. These penalties should be reviewed for consistency with the proposed new general secrecy offence and subsequent disclosure offence. In this regard, as discussed below, penalty benchmarks should be established and applied in drafting secrecy offences.

11.133 In the ALRC’s view, the maximum penalties for both the initial and subsequent unauthorised handling of Commonwealth information should be consistent, where the fault elements are the same and similar harm is caused by the conduct.

**Proposal 11–5** The penalties for specific secrecy offences should be reviewed for consistency with the general secrecy offence and the subsequent disclosure offence (Proposals 9–3 to 9–5), and in accordance with Proposals 11–7 to 11–11.

**Proposal 11–6** The maximum penalties for the initial and subsequent unauthorised handling of Commonwealth information under specific secrecy offences should generally be the same, subject to relevant differences in relation to fault elements or the reasonable likelihood of harm.

#### **Level of maximum penalty**

11.134 One mechanism by which the maximum penalties for specific secrecy offences might be made more consistent is through the application of benchmarks for particular categories of offences, to guide those who draft Commonwealth offence provisions.

168 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009; The Treasury, *Submission SR 22*, 19 February 2009.

169 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

170 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

### **Penalty benchmarks**

11.135 The *Guide to Framing Commonwealth Offences* states that relevant penalty benchmarks are to be taken into account in setting penalties for offences, and sets out penalty benchmarks for certain classes of offences.<sup>171</sup> The Guide specifies a penalty benchmark of two years imprisonment or 120 penalty units for breach of secrecy provisions—citing as examples provisions which relate to both initial<sup>172</sup> and subsequent<sup>173</sup> unauthorised disclosure of Commonwealth information.

11.136 The other benchmarks specified in the *Guide to Framing Commonwealth Offences* are relevant in gauging the relative criminality of secrecy offences compared with other Commonwealth offences. For example, the Guide specifies the same penalty benchmarks for breaching confidentiality requirements and for making false statements in applications for warrants.<sup>174</sup> It also sets out the following benchmarks:

- six months imprisonment or 30 penalty units for offences by witnesses;
- 50 to 60 penalty units for failure to lodge reports or returns;
- 12 months imprisonment or 60 penalty units for making false statements in notices or applications or failing to provide information that is required;
- five years imprisonment or 300 penalty units for corruption and abuse of public office; and
- life imprisonment for treason, certain war crimes and terrorist acts.<sup>175</sup>

### **Comparing penalties**

11.137 In assessing what levels of penalty should apply to particular secrecy offences, there is scope for comparing levels of penalty to proscribed conduct across different types of protected information. A value judgement about the comparative importance of protecting different types of information may be implicit in the levels of maximum penalties attached to the unauthorised handling of those types of information.

---

<sup>171</sup> Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 47.

<sup>172</sup> *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).

<sup>173</sup> *Australian Hearing Services Act 1991* (Cth) s 67(8).

<sup>174</sup> Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 47.

<sup>175</sup> *Ibid*, 47–48.

11.138 For example, under the *Aboriginal and Torres Strait Islander Act*, an officer of an ILC is subject to a maximum term of imprisonment for one year and a \$6,600 fine if he or she discloses information that is considered sacred or otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders; and the disclosure would be inconsistent with the views or sensitivities of those persons.<sup>176</sup> In contrast, as discussed above, the usual maximum penalty for disclosing confidential information is twice that level—two years imprisonment and a fine of \$13,200. In addition, the maximum penalty attaching to the unauthorised disclosure of information expected to affect adversely a person’s financial affairs<sup>177</sup> in some cases is greater than the penalty attaching to the unauthorised disclosure of sacred information.

11.139 It may also be asked whether, for example, it is appropriate that the maximum term of imprisonment for offences relating to disclosing information likely to prejudice the defence or security of Australia<sup>178</sup> or breaching orders made in the interests of the defence of Australia<sup>179</sup> is the same as those attaching to many offences concerning the disclosure of information related to the affairs of a person.<sup>180</sup>

### **Role of judicial discretion**

11.140 Both the Australian Parliament, in setting maximum penalties for offences, and sentencing courts play an important part in endeavouring to ensure that an appropriate type and level of penalty is imposed on an offender.

11.141 In sentencing a federal offender, s 16A(2) of the *Crimes Act* requires a court to take into account specified factors, to the extent that they are relevant and known. Among the factors that are to be considered are the ‘nature and circumstances of the offence’ and ‘any injury, loss or damage resulting from the offence’. Each of these factors is addressed below.

11.142 The ‘nature and circumstances’ of the offence would entail a consideration of, for example: the sensitivity of the information the subject of unauthorised conduct (for example, whether it was national security information); the type of conduct proscribed (for example, disclosure or mere receipt); and whether the conduct was intentional.<sup>181</sup>

11.143 The factor of ‘any injury, loss or damage resulting from the offence’ would entail a consideration of the consequences of breaching a secrecy provision; for example, whether the breach endangered life or safety, or prejudiced national security,

---

176 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S.

177 For example *Pooled Development Funds Act 1992* (Cth) s 71 (two years imprisonment and fine of \$13,200).

178 *Defence Force Discipline Act 1982* (Cth) s 58 (two years imprisonment).

179 *Designs Act 2003* (Cth) ss 108, 109; *Patents Act 1990* (Cth) s 173.

180 For example, *Taxation Administration Act 1953* (Cth) s 3C(2).

181 Such factors may also influence the determination by the Australian Parliament of the level of maximum penalty that should apply to secrecy offences.

an investigation, or a person's financial interests. Many secrecy offences do not contain an element of a likelihood of harm to an identifiable public interest. For such offences, the prosecution does not need to prove beyond reasonable doubt that harm did or was likely to ensue in order to establish criminal liability. However, where the conduct, in fact, harms the public interest, the fact and degree of harm are relevant aggravating factors to be considered in sentencing.

11.144 Some secrecy provisions, however, require proof that the unauthorised handling of Commonwealth information risked, or caused, harm to an identifiable public interest.<sup>182</sup> The degree of harm to the public interest would be a relevant factor in sentencing.

11.145 Finally, the *Defence Act 1903* (Cth) contains an anomalous penalty provision that allows a judge unfettered discretion with respect to the level of penalty that may be imposed for breach of s 73A of the Act ('Unlawfully giving or obtaining information as to defences'), when dealt with on indictment. Section 73F provides that this offence attracts a maximum penalty of imprisonment 'for any term' or a 'fine of any amount' or both.

### Short sentences of imprisonment

11.146 The ALRC has identified seven secrecy offences that specify maximum terms of imprisonment of three months.<sup>183</sup> Such penalties are contrary to the advice contained in the *Guide to Framing Commonwealth Offences*, which directs those framing Commonwealth offences to refrain from imposing terms of imprisonment of less than six months. It states that:

Avoiding provision for short term prison terms underlines the message that imprisonment is reserved for serious offences and also avoids the potential for burdening State/Territory correctional systems with minor offenders.<sup>184</sup>

11.147 In contrast, in *Same Crime, Same Time: Sentencing of Federal Offenders*, the ALRC recommended that sentences of imprisonment of less than six months should continue to be available in the sentencing of federal offenders.<sup>185</sup> The ALRC expressed the view that the federal sentencing regime protects against the inappropriate

---

182 See Ch 7.

183 *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32; *Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992* (Cth) s 25; *Defence (Inquiry) Regulations 1985* (Cth) regs 62, 63; *Commonwealth Functions (Statutes Review) Act 1981* (Cth) s 234; *Port Statistics Act 1977* (Cth) s 7; *Social Welfare Commission (Repeal) Act 1976* (Cth) s 8.

184 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 42–43.

185 Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), Rec 7–8.

imposition of short sentences.<sup>186</sup> The abolition of short sentences may have perverse consequences, resulting in offenders receiving longer sentences of imprisonment than would otherwise have been warranted.<sup>187</sup>

### **Submissions and consultations**

11.148 In IP 34, the ALRC asked whether there should be benchmarks for the maximum levels of criminal penalties that apply to secrecy offences and, if so, what should those benchmarks be. For example, should higher maximum penalties apply to offences involving the unauthorised handling of national security information, or an element of likelihood of harm to the public interest?<sup>188</sup>

11.149 Stakeholders supported the need for benchmarks.<sup>189</sup> PIAC and the Law Council submitted, for example, that benchmarks based on a categorisation of offences are needed to promote consistency. ASIC referred to the benchmarking approach taken in the *Guide to Framing Commonwealth Offences* as ‘an extremely useful tool’.<sup>190</sup>

11.150 The AGD noted that currently most secrecy offences carry a maximum penalty of two years imprisonment and that this ‘seems to be an appropriate penalty for the majority of secrecy offences’, adding that:

Generally, those secrecy offences involving particularly sensitive or national security information impose higher maximum penalties. The underlying principle for the imposition of higher maximum penalties in this latter category of offences is that there are certain types of Commonwealth information, the unauthorised disclosure of which could cause significant harm to the public interest and as such require additional protection. By its nature, the unauthorised disclosure of national security information will carry a higher likelihood of harm to the public interest. For example, national security information that has been received from sensitive sources such as foreign governments could not only damage international relations with that government but also jeopardise the security or defence of Australia.<sup>191</sup>

11.151 Stakeholders agreed that the provisions of the *Defence Act* allowing the imposition of a maximum penalty of imprisonment ‘for any term’ should be amended.<sup>192</sup> PIAC considered that it was not

---

186 As noted above, *Crimes Act 1914* (Cth) s 17A provides that a sentence of imprisonment should not be imposed for a federal offence unless the court is satisfied that no other sentence is appropriate in the circumstances of the case.

187 See Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), [7.70]–[7.72].

188 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–6.

189 For example, Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; Law Council of Australia, *Submission SR 30*, 27 February 2009.

190 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

191 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

192 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

appropriate, or of assistance in ensuring certainty, fairness and consistency of punishment as between similar offenders and offences, for a court to be given no guidance at all by the legislature as to the maximum penalty which is to apply to particular crimes.<sup>193</sup>

11.152 In this regard, the AGD also stated that:

It is generally not appropriate for an offence provision to fail to set a maximum penalty. A specified maximum penalty provides certainty and clarity in the maximum penalties an individual can face. It enables the public to readily see the seriousness and potential consequences of breaching a secrecy provision. A specified maximum penalty also provides guidance to the judiciary on sentencing levels deemed appropriate by the Australian Parliament for the offence.<sup>194</sup>

### ALRC's views

11.153 The starting point for achieving greater consistency should be the maximum penalties proposed for the new general secrecy offence: two years imprisonment for the first tier offence; and, for the other two tiers of the offence, where there is recklessness as to the reasonable likelihood of harm, five or seven years imprisonment, depending on the nature of the harm.<sup>195</sup>

11.154 In the ALRC's view, a maximum penalty of two years imprisonment and a fine of 120 penalty units is a reasonable benchmark—particularly given that a maximum penalty of two years imprisonment is consistent with more than 60% of existing secrecy offences. However, there is a need for a broader spectrum of penalty benchmarks, which reflect the ALRC's proposals on how the general and specific secrecy offences should generally be framed.

11.155 In particular, the ALRC proposes that specific secrecy offences should generally incorporate a requirement that, for an offence to be committed, there must be a reasonable likelihood that the disclosure of information will cause harm to some specified public interest.<sup>196</sup> The maximum penalty applying to secrecy offences which require a reasonable likelihood of harm should be higher than secrecy offences that do not contain such an element. Such an approach is currently taken under the *Surveillance Devices Act 2004* (Cth), which provides a maximum penalty of two years imprisonment for the unauthorised use, recording or disclosure of protected information;<sup>197</sup> and a maximum penalty of 10 years imprisonment where the same conduct ‘endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence’.<sup>198</sup>

<sup>193</sup> Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

<sup>194</sup> Attorney-General's Department, *Submission SR 36*, 6 March 2009.

<sup>195</sup> Proposal 9–3.

<sup>196</sup> Proposal 10–1.

<sup>197</sup> *Surveillance Devices Act 2004* (Cth) s 45(1).

<sup>198</sup> *Ibid* s 45(2).

11.156 Consistently with the more serious tiers of the general secrecy offence, a specific secrecy offence which requires that a person know, be reckless as to whether, or intend the disclosure of Commonwealth information to cause harm, should generally provide for a penalty of a maximum of five or seven years imprisonment. The level of penalty should depend on the nature of the harm. A lesser maximum penalty should apply where the interests being protected concern personal privacy; the business or professional affairs of a person; or the business, commercial or financial affairs of an organisation. As discussed in Chapter 9, while harm to these interests may have serious consequences, these would not usually involve risks to life or safety.

11.157 As discussed in Chapter 6, criminal penalties for disclosure of Commonwealth information should be reserved for serious offences, especially given that there are a range of other mechanisms in place to protect Commonwealth information, including administrative sanctions, contractual obligations and the general law. In the ALRC's view, the need for secrecy offences that are currently punishable by imprisonment for less than six months, or by pecuniary penalties only, should be reviewed and considered for repeal.

**Proposal 11–7** Guidance on benchmark penalties for specific secrecy offences, consistent with Proposals 11–8 to 11–11, should be incorporated into the Attorney-General's Department's *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*.

**Proposal 11–8** Subject to Proposals 11–9 and 11–10, specific secrecy offences should generally provide for a maximum penalty of two years imprisonment, or a pecuniary penalty not exceeding 120 penalty units, or both.

**Proposal 11–9** Specific secrecy offences should generally provide that, where a person knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:

- (a) have a substantial adverse effect on personal privacy; or
- (b) have a substantial adverse effect on a person in respect of his or her lawful business or professional affairs or on the business, commercial or financial affairs of an organisation,

the penalty should be a maximum of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both.

**Proposal 11–10** Specific secrecy offences should generally provide that, where a person knows, is reckless as to whether, or intends the disclosure of Commonwealth information to:

- (a) harm the national security, defence or international relations of the Commonwealth;
- (b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction, the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue;
- (c) endanger the life or physical safety of any person; or
- (d) pose a serious threat to public health or public safety

the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.

**Proposal 11–11** Specific secrecy offences that provide for maximum penalties of imprisonment for less than six months, or by pecuniary penalties only, should be reviewed and considered for repeal.



# **12. Specific Secrecy Offences: Simplification and Consistency**

---

## **Contents**

Introduction	413
Replication of secrecy offences	414
ALRC's views	415
Identifying examples of substantial replication	419
Examples of substantial replication	419
Case study: <i>Crimes Act 1914</i> (Cth) s 79	425
Consistency in secrecy offences	433
Submissions and consultations	433
ALRC's views	434
Consolidation of secrecy offences	436
Submissions and consultations	437
ALRC's views	438
Implementation	439
Drafting directions and guidance	440
ALRC's views	441

## **Introduction**

12.1 This chapter continues the focus on consistency in, and simplification of, specific secrecy offences by examining when specific secrecy offences may be considered to substantially replicate the proposed new general secrecy offence to be enacted in the *Criminal Code* (Cth) (the general secrecy offence).<sup>1</sup> The chapter examines the criteria involved in assessing whether there is substantial replication and identifies examples of offences that, subject to more detailed review, might be repealed on this basis.

12.2 The chapter also discusses concerns about lack of consistency in the drafting of specific secrecy offences and ways to address this problem, including through the consolidation of secrecy offences.

---

1     Discussed in Chs 6 to 9.

12.3 Finally, the chapter suggests a process for implementing reform of secrecy provisions, with a view to promoting more open government. Given the number of federal secrecy offences—there are more than 350—comprehensive review and reform will be an ongoing process requiring the involvement of many agencies of the Australian Government. This chapter develops proposals to ensure that this process is informed by the ALRC’s conclusions, primarily through the development of detailed drafting directions and other guidance against which existing and proposed specific secrecy offence provisions can be evaluated.

### **Replication of secrecy offences**

12.4 The Australian Government Attorney-General’s Department (AGD) *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers (Guide to Framing Commonwealth Offences)* states the principle that *Criminal Code* offences of general relevance to Commonwealth administration should not be replicated, and explains:

Broadly framed provisions of general application were placed in the *Criminal Code* to avoid the technical distinctions, loopholes, additional prosecution difficulty and appearance of incoherence associated with having numerous slightly different provisions to similar effect across Commonwealth law. There are also some provisions concerning offences in the *Crimes Act*. It is intended that these will be transferred to the *Criminal Code* in due course. Where a relevant *Criminal Code* or *Crimes Act* provision applies, separate provision should not be made in another Act.<sup>2</sup>

12.5 In its submission to this Inquiry, the AGD submitted that enacting a clarified and more targeted general secrecy offence in the *Criminal Code* ‘could result in greater reliance on the general offence, and consequently, fewer secrecy provisions being inserted in various Commonwealth Acts’. Further,

It would also tend to reduce the perceived need for including specific secrecy laws in other legislation on the basis that it is not sufficiently clear whether the general offence would apply, or to create a specific duty for the purpose of the general offence.<sup>3</sup>

12.6 It is Australian Government policy that *Criminal Code* offences of general relevance to Commonwealth administration should not be replicated in other laws. Therefore, new secrecy offences should not be enacted if they substantially replicate the proposed general secrecy offence in the *Criminal Code*.

12.7 In addition, any existing secrecy offences that replicate the general secrecy offence should be considered for repeal, as the opportunity arises. Such an approach

---

<sup>2</sup> Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 16.

<sup>3</sup> Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

would be consistent with the ALRC's function to review laws to, among other things, simplify the law and propose the repeal of obsolete or unnecessary laws.<sup>4</sup>

### ALRC's views

12.8 In practice, there is no secrecy offence that exactly replicates the terms of the proposed general secrecy offence. The main reason for this is that the proposed general secrecy offence requires that the disclosure be reasonably likely to cause harm to specified public interests—for example, if the disclosure is reasonably likely to prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences.<sup>5</sup>

12.9 Leaving aside the requirement for a reasonable likelihood of harm, the major respects in which the scope of existing specific secrecy provisions may differ from the general secrecy provision include where:

- the parties regulated extend beyond Commonwealth officers, as defined in the general secrecy provision;
- conduct other than the disclosure of information is covered—such as soliciting, receiving, obtaining, possessing, making a record of, or using information;
- the information protected includes information other than that to which a Commonwealth officer has, or had, access to by reason of being a Commonwealth officer;
- exceptions to a prohibition on disclosure differ significantly from those provided by the general secrecy offence; or
- penalties differ significantly from those provided by the general secrecy offence.

12.10 In practice, therefore, any review of existing provisions should examine whether specific secrecy offences can be identified that 'substantially replicate' the proposed general secrecy offence. An offence will do so when it is of such similar effect to the general secrecy offence that it is unnecessary and should be considered for repeal. The corollary is that secrecy offences should be retained where they differ in significant and necessary ways from the proposed general secrecy offence.

12.11 While the principle that secrecy offences should be repealed where they substantially replicate the proposed general secrecy offence is straightforward, identifying these offences is a complex task in practice. Specific secrecy offences

---

<sup>4</sup> Australian Law Reform Commission Act 1996 (Cth) s 21.

<sup>5</sup> See Ch 7.

differ in many and various respects from the general secrecy offence, and from each other.

12.12 The extent to which these differences alone may justify the retention of specific secrecy offences is discussed below. In practice, specific secrecy offences will differ from the general secrecy offence in more than one aspect, and usually in at least three or four.

#### ***Reasonable likelihood of harm***

12.13 The fact that a reasonable likelihood of harm test is not incorporated in a specific secrecy offence should not, of itself, mean that the offence should be retained where it otherwise substantially replicates the general secrecy offence.

12.14 For example, none of the secrecy offences in the *Aged Care Act 1997* (Cth)<sup>6</sup> require that a disclosure be reasonably likely to cause harm. There seems no reason to assume that the unauthorised disclosure of information of the type covered by these offences is, by its very nature, likely to cause harm.

12.15 As discussed in Chapters 7 and 10, the ALRC considers that criminal penalties are generally only justified where harm is reasonably likely to result from an unauthorised disclosure of Commonwealth information. Therefore, offences such as those in the *Aged Care Act* require some other significant and necessary difference from the general secrecy offence in order to justify retention.

#### ***Parties***

12.16 Some offences need to cover specific categories of parties, such as Pharmaceutical Benefits Scheme prescribers,<sup>7</sup> or participants in witness protection programs.<sup>8</sup> On this ground alone, such offences can be considered to differ in a significant and necessary way from the proposed general secrecy offence—and therefore to justify retention.

12.17 However, the fact that a specific secrecy offence extends to parties other than Commonwealth officers, as defined in the general secrecy offence, should not, of itself, mean that the offence should be retained where it otherwise substantially replicates the general secrecy offence—considered in conjunction with the subsequent disclosure offence.

12.18 Specific secrecy offences that are stated to apply to ‘any person’ should be reviewed for substantial replication of the general secrecy offence (in accordance with Proposal 10–3), where the information protected is defined as information acquired by the person in the course of performing duties or exercising powers or functions under

---

<sup>6</sup> *Aged Care Act 1997* (Cth) ss 86-2, 86-5 to 86-7.

<sup>7</sup> *National Health Act 1953* (Cth) s 135AAA(1).

<sup>8</sup> *Witness Protection Act 1994* (Cth) s 22(2).

specific legislation; or as information obtained for the purposes of specific legislation and held in the records of specific agencies (or similar formulations).

12.19 For example, the *Student Assistance Act 1973* (Cth) creates an offence applying to a person who discloses to any other person information that the person knows or ought reasonably to know is protected information.<sup>9</sup> ‘Protected information’ is defined, in summary, as information about a person that has been obtained for the purposes of this Act and is held in the records of the Department of Education, Employment and Workplace Relations (DEEWR) or Centrelink.<sup>10</sup>

12.20 In practice, it is questionable whether such an offence would ever apply to someone who is not a Commonwealth officer under the extended definition provided by the proposed general secrecy offence; or someone who knows or has reasonable grounds to believe that information has been disclosed by a Commonwealth officer in breach of the general secrecy offence—that is, a person covered by the proposed subsequent disclosure offence.

### **Conduct**

12.21 The fact that a specific secrecy offence extends to conduct other than the disclosure of information should not, of itself, mean that the offence should be retained where it otherwise substantially replicates the general secrecy offence.

12.22 In the ALRC’s view, while it may be appropriate in some contexts to criminalise other aspects of unauthorised information-handling, it is generally sufficient that such conduct as ‘making a record’ be the subject of administrative action, rather than a criminal offence.

12.23 Due to the operation of the *Criminal Code*, the fault element for the conduct elements of almost all specific secrecy offences is intention. The equivalent fault element in the proposed general secrecy offence is also intention, so inconsistency on this basis will be rare.

### **Information protected**

12.24 The information protected by specific secrecy offences that apply to Commonwealth officers is usually a subset of the information that would be covered by the general secrecy offence. The proposed general secrecy offence applies to all information to which a Commonwealth officer has, or had, access by reason of being a Commonwealth officer.

---

9        *Student Assistance Act 1973* (Cth) s 353.

10      Ibid s 3.

12.25 The fact that a specific secrecy offence is framed to protect a narrower category of information, therefore, should not of itself mean that the offence should be retained. For example, a secrecy offence in the *Gene Technology Act 2000* (Cth)<sup>11</sup> applies only to ‘confidential commercial information’ rather than to any information held by an officer of the Gene Technology Regulator by reason of being such an officer. As confidential commercial information to which a Commonwealth officer has access is covered by the general secrecy offence, there needs to be some other significant and necessary difference from the general secrecy offence in order to justify the retention of this specific offence.

### ***Exceptions and defences***

12.26 There are many reasons that specific secrecy offences have exceptions and defences that diverge from, or are more specific than, those in the general secrecy offence. In some cases, such offences can be considered to differ in a significant and necessary way from the proposed general secrecy offence—and justify retention.

12.27 However, whether a difference in applicable exceptions, of itself, justifies the retention of a specific secrecy offence needs to be assessed on a case by case basis. While some secrecy regimes justifiably involve detailed codification of authorised disclosure—for example, in the area of taxation—in other cases, where exceptions are more detailed or more specific than those set out in the general offence, the differences may not be significant.

12.28 For example, the secrecy offence contained in s 15 of the *AusCheck Act 2007* (Cth) provides for exceptions where disclosure is for the purposes of the AusCheck scheme; or to the AFP for the purposes of the AusCheck scheme. These exceptions, while specific, would be covered by the ‘in the course of an officer’s functions or duties’ exception contained in the proposed general secrecy offence and the defence of ‘lawful authority’ provided under the *Criminal Code*.<sup>12</sup>

12.29 In any case, more extensive provisions authorising certain specific uses and disclosures of information could be retained, even where the related secrecy offences themselves are repealed. For example, the circumstances in which the Secretary of the Department of Health and Ageing may disclose protected information set out in the *Aged Care Act 1997* (Cth)<sup>13</sup> could be retained, and inform the application of the exceptions that apply to the general secrecy offence and the application of IPP 11.1(d) of the *Privacy Act* to such disclosure.

---

11     *Gene Technology Act 2000* (Cth) s 187.

12     *Criminal Code* (Cth) s 10.5, applying where ‘the conduct constituting the offence is justified or excused by or under a law’.

13     *Aged Care Act 1997* (Cth) s 86-3.

### **Penalties**

12.30 The proposed general secrecy offence would attract a maximum penalty of seven years imprisonment. As discussed in Chapter 11, there is wide variation in the maximum penalties provided by specific secrecy offences and the ALRC proposes new penalty benchmarks, which also allow for a maximum penalty of seven years.

12.31 There may be some circumstances where specific secrecy offences merit or warrant a higher penalty.<sup>14</sup> If so, this might justify the retention of a specific secrecy offence, which would otherwise substantially replicate the general secrecy offence.

**Proposal 12–1** Commonwealth secrecy offences should generally be:

- (a) repealed where the scope of the offences substantially replicates the proposed general secrecy offence; and
- (b) retained where the offences differ in significant and necessary ways from the proposed general secrecy offence.

### **Identifying examples of substantial replication**

12.32 A number of specific secrecy offences may warrant repeal on the basis that the scope of the offences substantially replicates the proposed general secrecy offence. The following examples illustrate how these offences might be identified.

12.33 In each case, a secrecy offence provision is compared with the general offence provision across the main elements of the offences. The results are discussed in the text and summarised in a simple table. These examples should not, however, be taken as indicating that the ALRC has concluded that these secrecy offences should be repealed, if the new general secrecy offence proposed by the ALRC is implemented.

#### **Examples of substantial replication**

##### **Example 1: AusCheck Act 2007 (Cth) s 15**

###### **15 Protection of information**

- (1) A person commits an offence if:
  - (a) the person is or was an AusCheck staff member; and

<sup>14</sup> A small number of existing secrecy offences provide for a maximum penalty of more than seven years: eg, *Criminal Code* (Cth) s 91.1 (25 years imprisonment); *Defence Force Discipline Act 1982* (Cth) s 16 (15 years imprisonment); *Witness Protection Act 1994* (Cth) s 22(1) (ten years imprisonment).

- (b) when the person is or was an AusCheck staff member, the person obtained information relating to the AusCheck scheme; and
- (c) the person discloses the information to someone else.

Penalty: Imprisonment for 2 years.

(2) Each of the following is an exception to subsection (1):

- (a) a disclosure for the purposes of the AusCheck scheme;
- (b) if the information is AusCheck scheme personal information—a disclosure with the consent of the individual to whom the AusCheck scheme personal information relates;
- (c) if the information is AusCheck scheme personal information—a disclosure to the individual to whom the AusCheck scheme personal information relates;
- (d) a disclosure to the Australian Federal Police for the purposes of the AusCheck scheme.

12.34 The secrecy provision contained in s 15 of the *AusCheck Act 2007* (Cth) concerns the operation of the Australian Government entity that is responsible for identifying individuals who should not be eligible for an Aviation Security Identification Card or a Maritime Security Identification Card issued under transport security legislation.<sup>15</sup>

12.35 On balance, this provision appears to substantially replicate the general secrecy offence, leaving aside the reasonable likelihood of harm requirement.

12.36 AusCheck staff members are ‘Commonwealth officers’<sup>16</sup> as defined by the general secrecy offence; and the information protected is that to which a Commonwealth officer has, or had, access by reason of being a Commonwealth officer. There is no difference in the conduct and fault elements (disclosure and intention).

12.37 The exceptions contained in s 15(2)(a) and (d) would be covered by the ‘in the course of a Commonwealth officer’s functions or duties’ exception in the general secrecy offence; or the general defence relating to ‘conduct justified or excused by or under a law’ provided by the *Criminal Code*.<sup>17</sup> The ‘consent’ exceptions contained in s 15(2)(b) and (c) of the *AusCheck Act* do not replicate those in the general secrecy provision. It is doubtful whether this has any practical significance. Arguably, such disclosures would generally be made ‘in the course of a Commonwealth officer’s functions or duties’ and are permissible under the *Privacy Act 1988* (Cth).<sup>18</sup> In the

<sup>15</sup> *Aviation Transport Security Act 2004* (Cth); *Maritime Transport and Offshore Facilities Security Act 2003* (Cth).

<sup>16</sup> AusCheck operates as a division of the Australian Government Attorney-General’s Department.

<sup>17</sup> *Criminal Code* (Cth) s 10.5.

<sup>18</sup> *Privacy Act 1988* (Cth) s 14, IPPs 10, 11.

event that such disclosures are not within the functions or duties of officers, and are reasonably likely to cause harm, criminal penalties seem appropriate.

12.38 The penalty for contravention of the offence in s 15 is imprisonment for two years. This is the same as the penalty for the first tier of the general secrecy offence.

12.39 The results of a comparison with the elements of the general secrecy offence are summarised in the following table. A tick represents substantial replication between the offence and the proposed general secrecy offence, with respect to the relevant element of the offences. A dash represents no substantial replication.

<i>AusCheck Act 2007, s 15</i>	
<b>Element</b>	<b>Replication</b>
Likelihood of harm	—
Parties	✓
Conduct	✓
Fault	✓
Information protected	✓
Exceptions	—
Penalty	✓

#### **Example 2: Defence Act 1903 (Cth) s 73A(1)**

##### **73A Unlawfully giving or obtaining information as to defences**

(1) A person who is a member of the Defence Force or a person appointed or engaged under the *Public Service Act 1999* is guilty of an offence if:

- (a) the person communicates to any other person any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air force aerodrome or establishment or any other naval, military or air force information; and

- (b) the communication is not in the course of the first-mentioned person's official duty.

12.40 Again, on balance, this provision appears to substantially replicate the general secrecy offence, leaving aside the reasonable likelihood of harm requirement.

12.41 Members of the Defence Force and Australian Public Service employees are 'Commonwealth officers' and the information protected would generally be information to which a Commonwealth officer has, or had, access by reason of being a Commonwealth officer. There is no difference in the conduct and fault elements (disclosure and intention).

12.42 The exceptions contained in s 73A(1)(b) would be covered by the 'in the course of a Commonwealth officer's functions or duties' exception contained in the proposed general secrecy offence; or the general defence relating to 'conduct justified or excused by or under a law' provided by the *Criminal Code*.<sup>19</sup>

12.43 Section 73F states that:

- (2) The punishment for an offence under section 73A shall be:
- (a) if the offence is prosecuted summarily—a fine not exceeding \$200 or imprisonment for 6 months or both; or, in the case of a body corporate, a fine not exceeding \$2,000; or
  - (b) if the offence is prosecuted upon indictment—a fine of any amount or imprisonment for any term, or both.

12.44 The penalty provision under s 73F of the *Defence Act* is anomalous in that it allows a judge unfettered discretion with respect to the level of penalty that may be imposed, when dealt with on indictment.

12.45 The results of a comparison with the elements of the general secrecy offence can be summarised as follows:

<b><i>Defence Act 1903, s 73A(1)</i></b>	
<b>Element</b>	<b>Replication</b>
Likelihood of harm	—
Parties	✓

19      *Criminal Code* (Cth) s 10.5.

Conduct	✓
Fault	✓
Information protected	✓
Exceptions	✓
Penalty	—

**Example 3: *Chemical Weapons (Prohibition) Act 1994 (Cth)* s 102(2)****102 Secrecy**

(1) For the purposes of this section, an **eligible person** is a person who is or has been:

- (a) the Secretary to, or other officer of, the Department; or
- (b) the Director or the acting Director; or
- (c) a member of the staff referred to in section 88; or
- (d) engaged as a consultant to the Director; or
- (e) a national inspector; or
- (f) any other Commonwealth officer.

(2) Subject to this section, an eligible person must not either directly or indirectly, except for the purposes of this Act, for the purpose of complying with Australia's obligations under the Convention, or for the purpose of a prosecution for an offence against this Act:

- (a) make a record of, or divulge or communicate to any person, any confidential information concerning the affairs of another person acquired by the eligible person in the performance of duties in relation to this Act; or
- (b) produce to any person a confidential document relating to the affairs of another person given for the purposes of this Act; or
- (c) make a record of, or divulge or communicate to any person, any confidential information contained in the Register of Permits and Notifications.

12.46 On balance, this provision appears to substantially replicate the general secrecy offence, leaving aside the reasonable likelihood of harm requirement.

12.47 Any ‘eligible person’ under the Act would also be a ‘Commonwealth officer’ and confidential information acquired in the performance of duties in relation to the Act would generally be covered by the general secrecy offence. There is no difference in the conduct and fault elements (disclosure and intention).

12.48 The exceptions contained in s 102(2) would be covered by ‘in the course of a Commonwealth officer’s functions or duties’ and the general defence relating to ‘conduct justified or excused by or under a law’ provided by the *Criminal Code*.<sup>20</sup>

12.49 The penalty for contravention of the offence in s 102(2) is imprisonment for two years.<sup>21</sup> This is the same as the penalty proposed for the first tier general secrecy offence.

12.50 The results of a comparison with the elements of the general secrecy offence can be summarised as follows:

<i>Chemical Weapons (Prohibition) Act 1994 (Cth) s 102(2)</i>	
<b>Element</b>	<b>Replication</b>
Likelihood of harm	—
Parties	✓
Conduct	✓
Fault	✓
Information protected	✓
Exceptions	✓
Penalty	✓

20 Ibid s 10.5.

21 *Chemical Weapons (Prohibition) Act 1994* (Cth) s 102(3E).

### Case study: *Crimes Act 1914* (Cth) s 79

12.51 In Chapter 6, the ALRC proposes that s 79(3) of the *Crimes Act* be repealed and replaced, along with s 70, with a new general secrecy offence. Section 79 contains four other, narrower, secrecy offences, which are set out in s 79(2), (4), (5) and (6).<sup>22</sup>

12.52 The following section discusses whether these offences should be retained, repealed or replaced by new offences in the *Criminal Code*. In part, the answer to this question depends on the extent of any overlap between these offences and

- offences in s 91.1 of the *Criminal Code* dealing with espionage and similar activities (the espionage offences);<sup>23</sup> and
- the proposed new general secrecy offence.

12.53 A version of s 79 formed part of the first *Crimes Act* when enacted in 1914 and was based on provisions of the (now repealed) *Official Secrets Act 1911* (UK).<sup>24</sup> As noted in Chapter 5, when revising the espionage offences in 2001, the Government intended to repeal and replace s 79 with an updated offence in the *Criminal Code*.<sup>25</sup> The then Attorney-General, the Hon Daryl Williams AM QC MP, stated that the proposed updated provisions did not substantially change the law. However, there were some differences.<sup>26</sup> In particular, the proposed offence of ‘receiving information’ did not require the person to know, or have reasonable grounds to believe, that the information had been unlawfully communicated to them.<sup>27</sup> Following some criticism of the proposed offences, particularly by media organisations,<sup>28</sup> the Government withdrew these provisions of the amending Bill.

12.54 In 2004, the ALRC recommended that the Australian Government review s 79 to clarify and modernise the language and intent of the provision and to ensure that an appropriate public policy balance is found across the range of offences created by the provision.<sup>29</sup>

22 *Crimes Act 1914* (Cth) s 79 is set out in full in Appendix 5.

23 The espionage offences are described in Ch 5.

24 Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney-General), 265. See also Ch 5.

25 Criminal Code Amendment (Espionage and Related Offences) Bill 2001 (Cth).

26 R Sharman, ‘Espionage and Related Offences Bill’ (2002) 21(1) *Communications Law Bulletin* 7, 9. The explanatory memorandum stated that the Bill ‘substantially replicates section 79 of the *Crimes Act* except to the extent that Division 82 has been re-drafted to be consistent with rest of the *Criminal Code*’: Revised Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth), [25]. See also Ch 5.

27 Criminal Code Amendment (Espionage and Related Offences) Bill 2001 (Cth) cl 82.4.

28 R Sharman, ‘Espionage and Related Offences Bill’ (2002) 21(1) *Communications Law Bulletin* 7, 8.

29 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–4.

### ***Overlap with espionage offences***

12.55 As discussed in Chapter 6, the information protected by s 79 is, in part, defined by a circular concept—that is, information which, by its nature or the circumstances in which it is obtained, it is a person’s duty to keep secret. In addition, s 79(2), (4), (5) and (6) protect information

- made or obtained in contravention of Part VII of the *Crimes Act* (ie, in contravention of s 79 itself, or by ‘unlawful soundings’ prohibited by s 83);
- made or obtained in contravention of the espionage offences; or
- relating to a prohibited place or anything in a prohibited place.<sup>30</sup>

12.56 Information in these categories is likely to concern security and defence matters. In this regard, the offences in s 79 are similar to the espionage offences, which focus on the disclosure of information ‘concerning the Commonwealth’s security or defence’ to a foreign country or organisation with the intention of prejudicing the Commonwealth’s security or defence, or giving an advantage to another country’s security or defence.<sup>31</sup>

12.57 The secrecy offence most similar to the espionage offences is s 79(2), which concerns the disclosure or other handling of information with the intention of prejudicing the Commonwealth’s security or defence. However, s 79(2) has application to a broader category of information than the espionage offences, and does not require that the information was communicated, or was likely to be communicated, to a foreign country or organisation.

12.58 Section 79(4) makes it an offence for a person to:

- retain prescribed information ‘when he or she has no right to retain it or when it is contrary to his or her duty to retain it’;<sup>32</sup>
- fail to comply with a direction given by a lawful authority with respect to the retention or disposal of prescribed information;<sup>33</sup> or
- ‘fail to take reasonable care of [prescribed information] or to ensure that it is not communicated to a person not authorized to receive it or so conducts himself or herself as to endanger the safety of the information’.<sup>34</sup>

---

30     *Crimes Act 1914* (Cth) s 79(1)(a),(c). ‘Prohibited place’ is defined in *Crimes Act 1914* (Cth) s 80 and includes defence property and installations.

31     As discussed in Ch 5, there is also overlap between s 79 and s 70 of the *Crimes Act 1914* (Cth).

32     Ibid s 79(4)(a).

33     Ibid s 79(4)(b).

34     Ibid s 79(4)(c).

12.59 Sections 79(5) and (6) make it an offence to receive prescribed information knowing or having reasonable grounds to believe, at the time when he or she receives it, that it is communicated to him or her in contravention of the espionage offences or s 79(2) or (3).

12.60 These offences, like s 79(2), have application to a broader category of information than the espionage offences, and do not require that the information was communicated, or was likely to be communicated, to a foreign country or organisation. Unlike s 79(2), the offences do not require any intention to prejudice the security or defence of the Commonwealth.

#### ***Substantial replication of the general secrecy offence***

12.61 There is also some overlap between the offences in s 79 of the *Crimes Act* and the proposed general secrecy offence. Again, the similarity is greatest in the case of s 79(2).

12.62 The requirement for harm is similar—the proposed general secrecy offence refers to ‘damage to the security, defence or international relations of the Commonwealth’. The fault elements are the same: that is, intention with respect to the conduct and the likelihood of harm. The breadth of the information covered is similar.<sup>35</sup>

12.63 However, the s 79 offences are not confined in operation to Commonwealth officers, but apply to any person. The offences would nevertheless overlap in this respect with the proposed subsequent disclosure offence, which would apply where a person receives information knowing, or reckless as to whether, the information has been disclosed in breach of a secrecy offence, and then on-discloses the information knowing, or reckless as to whether, the disclosure would harm, or is reasonably likely to harm, a specified public interest.<sup>36</sup>

12.64 The offences in s 79 also refer to conduct—such as receiving, retaining and failing to comply with directions with respect to information—not covered by the general secrecy offence.

#### ***Submissions and consultations***

12.65 In IP 34, the ALRC asked whether, given the overlap between s 70 of the *Crimes Act*, s 79 of the *Crimes Act* and s 91.1 of the *Criminal Code*, any of the

---

35 That is, given the operation of s 79(1)(b), as discussed in Ch 5.

36 Proposal 8–3.

offences in s 79 should be replaced by updated offences in the *Criminal Code* and, if so, how should those offences be framed.<sup>37</sup>

12.66 The Law Council of Australia noted that the overlap between the provisions in the *Crimes Act* and the *Criminal Code* created uncertainty and stated that it

would like to see greater clarity in respect of the overlap and favours a repeal of the relevant *Crimes Act* secrecy provisions, with those offences incorporated in a modified form into the *Criminal Code*. This would reduce the uncertainty that currently exists.<sup>38</sup>

12.67 The AGD and the Australian Intelligence Community (AIC) agreed that there may be scope to review and consolidate the offences in ss 70 and 79 of the *Crimes Act* and s 91.1 of the *Criminal Code*.<sup>39</sup> However, both agencies were concerned to ensure that in consolidating the offences, the distinctive elements of each offence were preserved. The AIC submitted that ‘while there is some overlap between the three provisions, there are also important differences relating to the scope of each Act’ and that ‘it is essential to preserve each of the different aspects of the current provisions in any consolidation’.<sup>40</sup>

12.68 In particular, the AGD submitted that it was important to retain an offence like that in s 79(2), and that such an offence should not be limited to Commonwealth officers:

The offence at subsection 79(2) of the Crimes Act requires proof of an intention to prejudice the security or defence of the Commonwealth, and this offence carries a maximum penalty of 7 years imprisonment. It would seem important to retain an offence along this line, with a sufficiently high penalty, to act as a strong deterrent to anyone who might act with intention to prejudice national security or defence.<sup>41</sup>

12.69 The AGD also considered that there would be merit in retaining an offence like that in s 79(4) relating to the unauthorised retention or handling of certain documents and information, submitting that:

There would seem to be merit in retaining a provision along these lines, as it draws attention to the need to treat documents containing highly sensitive information with the highest degree of care to minimise the risk of inadvertent disclosure or unauthorised access.<sup>42</sup>

---

37 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 2–3.

38 Law Council of Australia, *Submission SR 30*, 27 February 2009.

39 Australian Intelligence Community, *Submission SR 37*, 6 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

40 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

41 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

42 Ibid.

***ALRC's views***

12.70 The offences in s 79(2), (4), (5) and (6) of the *Crimes Act* differ in two key respects from the proposed general secrecy offence. First, the *Crimes Act* offences apply to any person, rather than only to Commonwealth officers and, secondly, the *Crimes Act* offences cover conduct other than the unauthorised disclosure of information.

12.71 To the extent that conduct is not already covered by the espionage offences, these differences may justify the enactment of an updated offence derived from s 79. The ALRC proposes that aspects of s 79 should be incorporated in a new offence to be enacted in the *Criminal Code* (the proposed security offence).

***Proposed security offence***

12.72 In the ALRC's view, an offence similar in scope to that in s 79(2) is required to protect against the disclosure of information with an intention to prejudice the security or defence of the Commonwealth.

12.73 In the ALRC's view, it would be appropriate for the proposed security offence to cover a category of information similar to that protected by the espionage offences—that is, information ‘concerning the Commonwealth’s security or defence’.

12.74 This would mean that the scope of the proposed security offence is narrower than the offence in s 79(2). In the ALRC's view, however, it is unlikely that the unauthorised handling of information that does not, objectively, ‘concern’ security or defence would be capable of causing harm. In any case, where the person is a Commonwealth officer, the general secrecy offence may apply where there is disclosure with an intention to cause ‘damage to the security, defence or international relations of the Commonwealth’.

12.75 The expression ‘security or defence’ is defined in s 90.1 of the *Criminal Code* to include ‘the operations, capabilities and technologies of, and methods and sources used by, the country’s intelligence or security agencies’. A non-exhaustive list of information concerning security or defence could also be provided, including information:

- obtained in contravention of s 91.1 of the *Criminal Code*;
- concerning prohibited places; or
- obtained by unlawful soundings.

12.76 As discussed in Chapter 8, the ALRC considers that the proposed general secrecy offence should be limited to prohibiting the unauthorised disclosure of Commonwealth information. Other conduct, such as obtaining information, may be covered by the provisions in the *Criminal Code* where it is ancillary to the primary offence.<sup>43</sup>

12.77 In the ALRC's view, the focus of specific secrecy offences should also generally be on the disclosure of information, rather than on other conduct. In Chapter 10, the ALRC proposes that specific secrecy offences should generally not extend to conduct such as just making a record, receiving or possessing protected information.<sup>44</sup>

12.78 It may be appropriate to regulate other activity where the information concerns the security or defence of the Commonwealth. An analogy may be drawn with the espionage offences, which refer to a person who 'makes, obtains or copies a record'. In this area, it can be argued that it is necessary to criminalise acts preparatory to disclosure, to prevent harm to security or defence interests.

12.79 In the ALRC's view, the proposed security offence should cover situations where a person, without lawful authority and intending to prejudice the security or defence of the Commonwealth, *obtains* information concerning the Commonwealth's security or defence. An offence of this kind may apply where a person obtains such information other than by an unlawful disclosure by a Commonwealth officer.

12.80 The use of the word 'obtains' rather than 'receives', as used in the offences in s 79(5) and (6), is consistent with the wording of the espionage offences. While 'obtains' imports a more active role than 'receives', there may be no significant difference with s 79(5) and (6), because these offences are not committed where a person 'proves that the communication was contrary to his or her desire'.

12.81 Section 79(2)(c) makes it an offence for a person to fail to comply with a direction given by a lawful authority with respect to the retention or disposal of the information. Lawful directions may cover more than retention or disposal, and include requirements regarding the storage, copying or other handling of the information. The proposed security offence should provide that a person commits an offence if the person fails to comply with a direction given by a lawful authority with respect to the *use* of information concerning the Commonwealth's security or defence with the intention of prejudicing the Commonwealth's security or defence.

12.82 The proposed security offence should be located in pt 5.2 of the *Criminal Code*, which also contains the espionage offences. Consistently with the general secrecy offence and the penalty benchmarks proposed in Chapter 11, the offence should be punishable by a maximum penalty of ten years imprisonment and a fine of 600 penalty units.

---

43 See Ch 8.

44 Proposal 10–5.

12.83 There is considerable overlap between the proposed general secrecy offence and the proposed security offence. Circumstances would arise only rarely in which the proposed security offence would operate where the general secrecy offence (and associated subsequent disclosure offence) would not—for example, when:

- a person obtains information concerning the Commonwealth's security or defence but is not complicit in the disclosure of the information; or
- a person, other than a Commonwealth officer, discloses information concerning the Commonwealth's security or defence, which was not disclosed first by a Commonwealth officer, so that the subsequent disclosure offence does not operate.

12.84 Given this limited operation, the need for the proposed security offence may be challenged. The ALRC would welcome further comment on this point.

*Repeal of s 79*

12.85 In Chapter 6, the ALRC proposes that s 79(3) be repealed and replaced with the proposed general secrecy offence. For the reasons set out above, s 79(2) should also be repealed and replaced with the proposed security offence. The offences in s 79(4), (5) and (6) should also be repealed.

12.86 The offence in s 79(4) applies to various aspects of the unauthorised handling of information including where a person:

- retains the information;
- fails to comply with lawful directions with respect to the retention or disposal of the information; or
- fails to take reasonable care of the information or ensure it is not communicated.

12.87 While strict rules about the handling of national security classified information are necessary, s 79(4) may impose a criminal penalty on a person who: acts without an intention to cause harm to security or defence (or any other interest); inadvertently handles certain information; and may not be aware of the nature of the information.

12.88 The offence criminalises failing to ‘take reasonable care’ of information.<sup>45</sup> This is not an appropriate standard on which to base criminal liability and is inconsistent

---

45 Crimes Act 1914 (Cth) s 79(4)(c).

with the standard fault elements under the *Criminal Code* and guidance on framing criminal offences.<sup>46</sup>

12.89 At least some aspects of the conduct covered by s 79(4) would be addressed by the proposed security offence. For example, failure to comply with lawful directions—including those derived from the requirements of the *Australian Government Protective Security Manual* (PSM)<sup>47</sup>—with an intention to prejudice the Commonwealth’s security or defence, would constitute an offence.

12.90 There appears to be no justification for retaining the offences of receiving information currently set out in s 79(5) and (6) of the *Crimes Act*. It is difficult to identify the harm caused by the mere receipt of information, particularly as there is no need to show that the person intended to use the information in any way. The ALRC notes in this regard that the *Official Secrets Act 1989* (UK), which replaced the UK equivalent of s 79 in the *Official Secrets Act 1911* (UK), does not make receipt of official information an offence.<sup>48</sup>

12.91 Further, soliciting or receiving information from a Commonwealth officer in contravention of the proposed general secrecy offence may be an ancillary offence such as aiding and abetting or procuring the commission of the proposed general secrecy offence. Part 11 of the *Criminal Code* provides that a person guilty of an ancillary offence set out in that part is guilty of the offence itself.

**Proposal 12–2** Section 79 of the *Crimes Act 1914* (Cth) should be repealed and a new provision inserted in the *Criminal Code* (Cth) making it an offence for a person, without lawful authority and intending to prejudice the Commonwealth’s security or defence, to:

- (a) disclose or obtain information concerning the Commonwealth’s security or defence; or
- (b) fail to comply with a direction given by a lawful authority with respect to the use of information concerning the Commonwealth’s security or defence.

The offence should be punishable by a maximum penalty of ten years imprisonment and a fine of 600 penalty units.

46 Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 4.4.

47 Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM)* (2005).

48 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), [232]–[233].

## Consistency in secrecy offences

12.92 Concern has long been expressed about the number and diversity of Commonwealth secrecy provisions and the lack of consistency in the drafting of offences and associated penalties.<sup>49</sup> The Terms of Reference for this Inquiry refer to the desirability of having consistent laws and practices in relation to the protection of Commonwealth information.<sup>50</sup>

### Submissions and consultations

12.93 Stakeholders highlighted a range of concerns about lack of consistency and unwarranted complexity in existing secrecy laws. The Department of Human Services (DHS) examined the extent to which there is divergence in secrecy laws directly relevant to its responsibilities. The DHS provided detailed information highlighting significant inconsistencies in secrecy provisions across 12 statutes.<sup>51</sup> Some of the inconsistencies were summarised as follows:

In relation to coverage, for example:

- 4 out of 12 laws regulate uses by employees;
- 9 out of 12 regulate collections (or ‘making records’) by officers (the *Health Insurance Act* and *National Health Act* differ in this regard);
- 10 out of 12 have provision for public interest certificates (all but those relating to [the Child Support Agency]); and
- 6 out of 12 are referenced in Schedule 3 of the FOI Act.

Penalties also vary across the portfolio. For example, the penalty for an employee disclosing (however termed) protected information ranges from \$500 (*Health Insurance Act*) to 2 years imprisonment and 120 penalty units (\$13,200 at the time of writing) (*Dental Benefits Act*). Medicare Australia advises that the information protected under the *Health Insurance Act* and the *Dental Benefits Act* is essentially the same.<sup>52</sup>

12.94 The DHS noted that inconsistency creates a number of complications, including where agencies share information in circumstances where the disclosing agency’s secrecy obligations follow the information and the receiving agency’s secrecy obligations also apply to the collection or recording of the information. Further,

<sup>49</sup> For example, see Australian Parliament—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), 95, 118.

<sup>50</sup> The Terms of Reference are set out at the front of this Discussion Paper.

<sup>51</sup> *Dental Benefits Act 2008* (Cth); *Medical Indemnity Act 2002* (Cth); *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth); *Social Security (Administration) Act 1999* (Cth); *Aged Care Act 1997* (Cth); *Australian Hearing Services Act 1991* (Cth); *Child Support (Assessment) Act 1989* (Cth); *Child Support (Registration and Collection) Act 1988* (Cth); *Disability Services Act 1986* (Cth); *Student Assistance Act 1973* (Cth); *Health Insurance Act 1973* (Cth); *National Health Act 1953* (Cth).

<sup>52</sup> Department of Human Services, *Submission SR 26*, 20 February 2009.

There is also the potential for misunderstanding and confusion where one employee provides services or advice on behalf of more than one portfolio agency, or where one agency seeks information from another agency which is regulated by a different set of secrecy laws. Often secrecy laws require a deal of experience and understanding in the agency's particular context, and customers and officers from other agencies may have difficulty understanding their operation in particular circumstances or where the variations between the regimes are subtle. A coordinated and more consistent approach would be beneficial.<sup>53</sup>

12.95 The Social Security Appeals Tribunal (SSAT) also highlighted difficulties in dealing with multiple secrecy provisions:

The SSAT's jurisdiction extends across the areas of social security, family assistance, student assistance and child support. Each of these jurisdictional areas is subject to various legislative enactments and each of these enactments [and attendant regulations] has within it a series of secrecy/confidentiality provisions which add a further layer to the requirements imposed upon the SSAT by the privacy legislation.<sup>54</sup>

12.96 The SSAT referred, in particular, to widely varying definitions of the information protected by different secrecy laws:

Some of these definitions are extremely broad, such as the definition of 'protected information' in our child support jurisdiction and, like the definition of 'personal information' in the *Privacy Act*, catch virtually all information that can identify a person. Alternatively, the definition of 'protected information' in our social security/family assistance jurisdictions is extremely narrow and catches only information that is, or was, held in certain enumerated agencies and departments. Certain of this information may be disclosed to the appropriate authorities; other information cannot be so disclosed. Other sorts of information are tied to the prejudicial effect to the working of government, or where the information is received in confidence. Some provisions catch our tribunal members; whereas, other provisions catch only our APS staff. Some provisions catch everyone. So, overall, the plethora of provisions and definitions give rise to a great deal of confusion and difficulty of application.<sup>55</sup>

### **ALRC's views**

12.97 Specific secrecy offences vary in many ways, some more justifiable than others. Chapters 10 and 11 discuss how specific secrecy offences should be framed in order to be more consistent with the proposed new general secrecy offence, and with each other, and highlights aspects of the general secrecy offence that might usefully be more broadly adopted.

12.98 In this context, the ALRC makes a number of proposals intended to guide the framing of specific secrecy offences. These proposals provide that specific secrecy offences:

---

53 Ibid.

54 Social Security Appeals Tribunal, *Submission SR 14*, 17 February 2009.

55 Ibid.

- should generally incorporate a requirement that, for an offence to be committed, there must be a reasonable likelihood that the disclosure of information will cause harm to some specified interest (Proposal 10–1);
- incorporating a reasonable likelihood of harm requirement, should generally have recklessness as the fault element for more serious offences (punishable by imprisonment for more than a maximum of two years), and for other offences, strict liability should apply in relation to the likelihood of harm (Proposal 10–2);
- that are stated to apply to ‘any person’, should be reviewed to establish whether the offences should apply only to ‘Commonwealth officers’ and subsequent disclosure, as defined in the general secrecy offence and the subsequent disclosure offence (Proposal 10–3);
- that apply to Commonwealth officers, should be reviewed to establish whether the offences should be stated to apply also to former Commonwealth officers (Proposal 10–4);
- should generally not extend to conduct other than the disclosure of information, such as making a record, receiving or possessing protected information (Proposal 10–5), and should generally require intention as the fault element for the disclosure of information (Proposal 10–6);
- that specify that strict liability applies to one or all physical elements should be reviewed to establish whether the application of strict liability remains justified (Proposal 10–7);
- that apply to Commonwealth officers, should generally apply to all information to which a Commonwealth officer has, or had, access by reason of being a Commonwealth officer (Proposal 10–8);
- that include defences, should be reviewed, in accordance with the proposals in Chapter 11, to assess whether these defences are appropriate, in view of the general principles of criminal responsibility set out in ch 2 of the *Criminal Code*. Where such a defence is found to be appropriate, consideration should be given to recasting the provision as an exception, rather than as a defence (Proposal 11–1);
- that include extensive codification of permissible disclosure, should be reviewed to establish whether these exceptions are necessary or desirable (Proposal 11–2);

- that apply to Commonwealth officers, should generally be accompanied by a note cross-referencing the immunity provided by Commonwealth public interest disclosure legislation (Proposal 11–3);
- should be reviewed to ensure that penalties are consistent with the general secrecy offence and the subsequent disclosure offence, in accordance with Proposals 11–4 to 11–11.

12.99 Review of secrecy offences against these criteria would, in the ALRC’s view, significantly improve the consistency of secrecy offences, reduce complexity and make the law more accessible. In addition, the consolidation of secrecy offences should be considered, as discussed below.

### **Consolidation of secrecy offences**

12.100 Consolidation is another mechanism by which to promote consistency in, and simplification of, specific secrecy offences. This may involve consolidating secrecy provisions in the same legislation into a single provision or division in that Act or regulation. Secrecy provisions also may be consolidated across a number of pieces of legislation, such as those administered by the same agency.

12.101 While many Acts contain a single consolidated provision, division or part dealing with secrecy or confidentiality, a different approach has been adopted in some cases. The *Veterans’ Entitlements Act 1986* (Cth), for example, contains a number of secrecy provisions in similar terms dealing with the disclosure of confidential information in determinations in relation to different entitlements.<sup>56</sup> This approach appears to give rise to unnecessary duplication.

12.102 The proposed consolidation of taxation secrecy and disclosure provisions is an example of the second form of consolidation. In 2006, the Treasury undertook a review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review).<sup>57</sup> In its discussion paper, the Treasury noted that taxation secrecy provisions are located in numerous different Acts, differ in their language and scope, and have inconsistent penalties.<sup>58</sup> Further, it noted that some provisions merely duplicate provisions located in other Acts.<sup>59</sup>

12.103 The Taxation Secrecy Review proposed that the secrecy and disclosure provisions across all laws administered by the Commissioner of Taxation (including laws governing superannuation, excise, and Australian Business Number and Tax File

---

<sup>56</sup> *Veterans’ Entitlements Act 1986* (Cth) ss 35H(7)(a), 36L(8)(a), 37L(8)(a), 38L(8)(a), 45Q(8)(a).

<sup>57</sup> The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006).

<sup>58</sup> *Ibid.* [2.1].

<sup>59</sup> *Ibid.*

Number disclosures) be standardised and consolidated into a single piece of legislation.<sup>60</sup>

12.104 In March 2009, the Assistant Treasurer and Minister for Competition Policy and Consumer Affairs, the Hon Chris Bowen MP, released for public consultation an exposure draft Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill (Tax Laws Exposure Draft Bill). The Tax Laws Exposure Draft Bill proposes to consolidate, into a single comprehensive framework within the *Taxation Administration Act 1953* (Cth), taxation secrecy and disclosure provisions that are currently found across 18 pieces of taxation legislation.

12.105 In IP 34, the ALRC asked whether secrecy provisions should be consolidated, wherever possible, into a single provision in each Act or regulation.<sup>61</sup> The ALRC also asked whether, given that the consolidation of taxation secrecy laws is being considered, there are other legislative areas in which consolidation would be appropriate.<sup>62</sup>

### Submissions and consultations

12.106 Stakeholders agreed that, where possible, secrecy provisions should be consolidated, but emphasised that consolidation is not always appropriate.<sup>63</sup> DEEWR, for example, stated that:

To assist with clarity, avoid confusion and minimise the length of an Act or regulation, it would be highly desirable, where possible, for secrecy provisions to be consolidated into a single provision.

Additionally, where it is suitable and possible, the Department recognises the benefits in having a level of consistency in secrecy provisions across different legislative frameworks. However, caution should be exercised to avoid standardising secrecy provisions simply for the sake of it, as differing contexts are likely to necessitate some level of disparity.<sup>64</sup>

12.107 The Treasury outlined some of the reasons why consolidation was considered appropriate for taxation secrecy and disclosure provisions:

- All the provisions are obviously administered by the same agency.

---

60 Ibid, [2.3].

61 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 2–7.

62 Ibid, Question 2–4.

63 For example, Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

64 Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009.

- While the provisions do vary to some extent, there are general principles common to all provisions.
- It is consistent with a broader initiative to consolidate existing taxation administrative provisions into a single piece of legislation.<sup>65</sup>

12.108 The AIC stated that it supported ‘simplicity and transparency in the principles that drive protection’ and acknowledged that ‘consolidation of existing secrecy provisions could simplify arrangements’. However, the AIC did not support ‘the updating or consolidation of secrecy laws where this would reduce the current protections’. In particular, the AIC considered that:

there is no need to consolidate the secrecy provisions set out in the *Crimes Act*, the *Criminal Code*, the *Intelligence Services Act* and the ASIO Act into single provisions in each Act. In contrast to the example of the *Veterans Entitlements Act 1986*, cited in the Issues paper, these provisions are set out clearly and logically, in the context of those Acts.<sup>66</sup>

12.109 The Australian Commission for Law Enforcement Integrity stated that it ‘prefers a situation where the main secrecy provisions that apply to law enforcement agencies are retained in each agency’s principal statute’. Similarly, the DHS noted that:

Most portfolio agencies expressed a preference for maintaining the existing separate secrecy laws and noted that any moves towards greater consistency (for example, by one portfolio wide legislative provision) should not detract from the capacity of the applicable secrecy laws to respond to the particular needs and functions of each agency.<sup>67</sup>

12.110 The AGD observed that, while consolidation of secrecy laws may help to reduce complexity in some cases, this will depend upon the objectives and overall drafting of each Act:

By way of example, the *Australian Security Intelligence Organisation Act 1979* contains a number of secrecy provisions, which would not seem to benefit significantly by consolidating them into a single provision or a single part of the Act. In particular, section 34ZS contains a secrecy offence that relates specifically to a particular type of warrant. It would not be very logical to remove it from Division 3 of Part III of the Act and place it with other secrecy offences, as it would be separated from the provisions to which it directly relates.<sup>68</sup>

### **ALRC’s views**

12.111 In some instances, consolidation of secrecy offences within a statute may be desirable in order promote consistency and accessibility of law. On the other hand, the AGD *Guide to Framing Commonwealth Offences* sets out the principle that offences should generally be located with other provisions with the same substantive subject

---

65 Australian Taxation Office, *Submission SR 13*, 16 February 2009.

66 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

67 Department of Human Services, *Submission SR 26*, 20 February 2009.

68 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

matter, rather than being grouped together in an ‘Offences’ part. The Guide explains this principle as follows:

The placement of offences with related substantive provisions assists the reader to identify and understand the relationship between the two. Where provisions are separate, the offence provision and substantive provisions should explicitly refer to each other, so that those subject to the law and those administering the law can readily ascertain the relationship between the provisions.<sup>69</sup>

12.112 The Taxation Secrecy Review provides a good model for consolidation of secrecy provisions across a number of statutes administered by the same agency or agencies. This kind of exercise might usefully be repeated, for example, in relation to secrecy provisions contained in human services legislation.

**Proposal 12–3** The Australian Government should review Commonwealth secrecy offences that are retained with a view to consolidation, where possible, into:

- (a) a single provision or part where multiple secrecy provisions exist in the same Act;
- (b) one Act where multiple secrecy provisions exist in more than one Act for which the same Australian Government agency is, or agencies are, responsible.

## Implementation

12.113 Implementation of the ALRC’s proposals for reform of specific secrecy offences will be a lengthy and complex process. The elements of each specific secrecy offence need to be analysed in the light of each proposal and the role and purpose of the secrecy offence.

12.114 The ALRC does not expect the Australian Government—assuming that it agrees with the conclusions of the ALRC’s final Report in this Inquiry—to introduce an ‘omnibus’ secrecy offences reform bill dealing with changes to secrecy offences across the Commonwealth statute book. Rather, it is anticipated that there will be ongoing review of secrecy offences, as the opportunity arises.

12.115 In some cases, an agency may undertake a review of secrecy offences across the statutes for which the agency has responsibility or across a portfolio or functional

<sup>69</sup> Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 13.

area—as in the case of the recent review of taxation secrecy and disclosure provisions undertaken by Treasury.<sup>70</sup> In other cases, review might be more ‘opportunistic’—such as when amendments to legislation are being contemplated, making it convenient to review and amend a related secrecy provision; or where new legislation is being drafted.

### Drafting directions and guidance

12.116 One means to ensure that the recommendations of the Final Report of this Inquiry are taken into account when secrecy provisions are being reviewed or drafted is through the issuing of drafting directions or other guidance.

12.117 The AGD provides guidance relevant to the drafting of secrecy offences. The Department is responsible for assisting the Attorney-General to ensure that criminal law enforcement provisions are framed in a sound, effective and coherent manner. The AGD scrutinises all offence, civil penalty and law enforcement provisions in proposed legislation and provides policy advice and assistance to instructing agencies in tailoring these provisions.<sup>71</sup> As part of this role the AGD has produced the *Guide to Framing Commonwealth Offences*.<sup>72</sup> The Guide contains general advice on, for example, not replicating *Criminal Code* offences, separating the physical elements of offences, and using standard fault elements.

12.118 Drafting Directions are instructions issued by First Parliamentary Counsel, the head of the Office of the Parliamentary Counsel (OPC). The OPC is established under the *Parliamentary Counsel Act 1970* (Cth) and its principal functions are drafting bills for introduction into either House of the Parliament and drafting amendments of bills. All drafters are required to comply with the directions, which ensures that a consistent approach is taken to amendments.

12.119 Current drafting directions cover a wide range of topics, including some limited aspects of drafting secrecy provisions. *Drafting Direction No. 3.5* deals with offences, penalties, self-incrimination, secrecy provisions and enforcement powers. This direction provides that secrecy provisions should take into account the possibility that information may be the subject of inquiry by the Parliament or a parliamentary committee and that, in such cases, the secrecy provision should specify the circumstances in which information may be disclosed to the Parliament or parliamentary committee.<sup>73</sup>

---

70 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006); Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth).

71 See Attorney-General’s Department, *Criminal Law* (2009) <<http://www.ag.gov.au>> at 14 April 2009.

72 For example, Australian Government Attorney-General’s Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007).

73 Parliamentary Counsel, *Drafting Direction No. 3.5: Offences, Penalties, Self-Incrimination, Secrecy Provisions and Enforcement Powers*, Office of Parliamentary Counsel, 13 November 2007, [58]–[62].

12.120 The OPC's *Drafting Direction No. 3.5* states that legislative drafters should have regard to the *Guide to Framing Commonwealth Offences* in drafting provisions covered by the Guide, but should bear in mind that 'the Guide is neither binding nor conclusive, and that Commonwealth criminal law policy necessarily develops in response to changes in Government policy, novel legal issues, and emerging enforcement circumstances'.<sup>74</sup>

12.121 The ALRC noted in IP 34 that the options for reform of secrecy provisions include the development of guidance on whether it is appropriate to introduce or retain a secrecy provision in federal legislation and model secrecy provisions to assist in drafting future Commonwealth secrecy laws. In response, the AGD stated that:

Although it is probably not possible or desirable to formulate a single model secrecy provision, there would certainly seem to be scope for greater consistency between secrecy provisions which seek to achieve a similar purpose.<sup>75</sup>

### ALRC's views

12.122 In *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC recognised that 'a certain amount of flexibility across the range of Commonwealth secrecy provisions is acceptable', but expressed concern about the lack of consistency in the fundamental principles underpinning the provisions.<sup>76</sup>

12.123 The proposals made by the ALRC in this Discussion Paper are intended to establish a principled basis for review of existing secrecy provisions, based on an understanding of the appropriate relationship between the interests protected by secrecy and interests in open and accountable government. This understanding is reflected in the proposed framing of the new general secrecy offence.

12.124 In the ALRC's view, the proposed new general secrecy offence provides an appropriate model for the framing of secrecy offences. Specific secrecy offences should be framed in order to be consistent, as far as possible, with the general secrecy offence and with each other. Significant departures from the approach taken in the general secrecy offence need to be justified.

12.125 There is need, in this regard, for both general policy guidance, including in relation to when the enactment of specific secrecy offences may be justified, and more detailed drafting advice. The *Guide to Framing Commonwealth Offences*—or a new AGD guide dealing specifically with secrecy offences—would be an appropriate

---

74 Ibid, 3.

75 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

76 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [5.118].

source of guidance to be used by agencies early in the development of legislative proposals.

12.126 OPC Drafting Directions could draw from this document to provide more detailed directions aimed at technical drafting matters, giving effect to the desired policy framework. For example, the ALRC has proposed that the OPC should issue Drafting Directions requiring that any proposed:

- secrecy provision should indicate expressly whether it overrides the *Freedom of Information Act 1982* (Cth) (Proposal 4–2); and
- non-disclosure provision should indicate expressly whether it overrides the *Archives Act 1983* (Cth) in the open access period (Proposal 4–7).

12.127 In conjunction with the development and publication of guidance on when the enactment of specific secrecy offences is justified and how such offences should be framed, the AGD should have a role in encouraging the proposed ongoing review of existing secrecy offences.

**Proposal 12–4** The Australian Government should review Commonwealth secrecy offences that are retained for consistency with the proposed general secrecy offence, in accordance with Proposals 10–1 to 10–8, 11–1 to 11–11, 12–1 and 12–3.

**Proposal 12–5** The Attorney-General’s Department should incorporate guidance in the *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* dealing with:

- (a) the circumstances in which the enactment of a specific secrecy offence may be justified;
- (b) the drafting of secrecy provisions so that specific secrecy provisions are consistent with, and do not replicate the scope of, the general secrecy offence.

This guidance should incorporate the drafting advice contained in Proposals 10–1 to 10–8, 11–1 to 11–11, 12–1 and 12–3.

# 13. Administrative Obligations in the Australian Public Service

---

## Contents

Introduction	443
The Australian Public Service	444
Framework for secrecy obligations in the APS	445
Secrecy obligations under the general law	445
Secrecy obligations under the <i>Public Service Act</i>	447
Role for secrecy provisions in the <i>Public Service Act</i>	448
Relationship between secrecy obligations and other APS requirements	449
Prejudice to the effective working of government	450
Background	450
Submissions and consultations	453
Options for reform	454
ALRC's views	459
Information communicated in confidence	464
Background	464
Duplicating 'harm to the effective working of government'?	464
ALRC's views	465
Exceptions and defences	466
Background	466
ALRC's views	468
Penalties	469
Background	469
Submissions and consultations	470
ALRC's views	471
Processes for dealing with breaches	472
Background	472
Submissions and consultations	478
ALRC's views	479

## Introduction

13.1 The administrative setting is the context in which persons employed by an Australian Government agency will most commonly interact with obligations of secrecy. The employment relationship imposes secrecy obligations on Commonwealth employees, breach of which may give rise to administrative disciplinary penalties. The

information-handling policies and practices of Australian Government agencies set the framework for how employees and others interpret and comply with these obligations of secrecy. For persons that deal with Australian Government agencies other than in an employment relationship, contractual provisions may impose obligations of secrecy.

13.2 The following three chapters of this Discussion Paper focus on the administrative secrecy framework in the Australian Government. This chapter considers the administrative secrecy obligations of persons engaged as Australian Public Service (APS) employees under the *Public Service Act 1999* (Cth), and makes a number of proposals for clarifying and consolidating these obligations. Procedural safeguards for the investigation and enforcement of administrative secrecy obligations are also discussed.

13.3 Chapter 14 proposes models for harmonising the administrative secrecy regimes that apply to Commonwealth employees other than APS employees—such as members of the Australian Defence Force, members of the Australian Federal Police (AFP) and employees of public authorities—with the *Public Service Act* framework. The chapter also considers mechanisms for regulating persons who are not in an ongoing employment relationship with the Australian Government, such as private sector contractors and former Commonwealth employees.

13.4 Chapter 15 discusses the tools available to Australian Government agencies to foster effective information-handling practices; for example, through developing and implementing information-handling policies and engaging employees in training and development programs.

## The Australian Public Service

13.5 The *Public Service Act* provides the legislative framework for the APS. The APS is defined in s 7 of the Act as comprising agency heads and employees of:

- Commonwealth departments of State;
- executive agencies established by the Governor-General under s 65 of the *Public Service Act*,<sup>1</sup> and

---

<sup>1</sup> Executive agencies include, eg, the Bureau of Meteorology; CrimTrac Agency; Insolvency and Trustee Service Australia; National Archives of Australia; and Old Parliament House: Australian Public Service Commission, *Australian Public Service Agencies* (2009) <[www.apsc.gov.au/apsprofile/agencies.htm](http://www.apsc.gov.au/apsprofile/agencies.htm)> at 31 March 2009.

- statutory agencies, being bodies declared by an Act to be a statutory agency for the purposes of the *Public Service Act*.<sup>2</sup>

13.6 As at June 2008, more than 160,000 people were engaged as APS employees,<sup>3</sup> with employees and agencies covered by the *Public Service Act* accounting for over two-thirds of the Commonwealth public sector.<sup>4</sup>

## Framework for secrecy obligations in the APS

### Secrecy obligations under the general law

13.7 Aspects of the general law impose duties on employees (including APS employees) not to disclose information in certain circumstances where this would be contrary to the wishes of their employer. As discussed in Chapter 5, general law obligations include: the equitable doctrine of breach of confidence, the duty of fidelity and loyalty, and the contractual requirement for employees to obey ‘lawful and reasonable directions’ issued by their employer. These may supplement the statutory secrecy obligations that apply to APS employees, discussed later in this chapter.

#### *Breach of confidence*

13.8 The elements of an action for breach of confidence are discussed in detail in Chapter 5. As noted in that chapter, the general principle is that the court will restrain the publication of confidential information where it has been obtained improperly or surreptitiously, or where the information imparted in confidence ‘ought not to be divulged’.<sup>5</sup> This doctrine may be invoked to restrain an APS employee from disclosing Commonwealth information in certain situations.<sup>6</sup> An injunction will only be awarded, however, where the court determines that the disclosure would be likely to injure the public interest. The mere fact that the disclosure would expose the government to public discussion and criticism is not sufficient to enliven the doctrine.<sup>7</sup>

#### *Duty of fidelity and loyalty*

13.9 As discussed in Chapter 5, under the common law, every employee is subject to a duty of fidelity and loyalty (or good faith). The duty of fidelity has largely been imposed in situations involving confidential information and has been expressed as requiring an employee not to use information obtained in the course of his or her

2 Statutory agencies may employ all of their staff under the *Public Service Act 1999* (Cth), as is the case, for example, with the Administrative Appeals Tribunal, the Australian Competition and Consumer Commission, the Australian National Audit Office, Centrelink and Medicare Australia. Other statutory agencies, such as the Australian Bureau of Statistics and the Australian Electoral Commission have dual staffing powers under the *Public Service Act* and another Act: Australian Public Service Commission, *Australian Public Service Agencies* (2009) <[www.apsc.gov.au/apsprofile/agencies.htm](http://www.apsc.gov.au/apsprofile/agencies.htm)> at 31 March 2009.

3 Australian Public Service Commission, *State of the Service Report 2007–08* (2008), 16.

4 Ibid, 2. This figure excludes permanent members of the Australian Defence Force.

5 *Commonwealth v Fairfax* (1980) 147 CLR 39.

6 Damages or an account of profits may also be available.

7 *Commonwealth v Fairfax* (1980) 147 CLR 39, 52.

employment to the detriment of the employer.<sup>8</sup> A further incident of the duty is compatibility between an employee's conduct and the necessary confidence between employer and employee.<sup>9</sup>

13.10 In *Bennett v President, Human Rights and Equal Opportunity Commission* ('Bennett'), Finn J noted there was little judicial consideration of the way in which the duty applies to 'the distinctive demands of public sector employment' in the Australian context.<sup>10</sup> Finn J advised, however, that any such consideration would need to take into account 'the precepts of loyalty, neutrality and impartiality which are hallmarks of a public service in a system of responsible government'.<sup>11</sup>

#### **Duty to obey lawful and reasonable directions**

13.11 Another aspect of an employee's duties that may give rise to a particular obligation of confidentiality is the requirement on every employee to obey lawful and reasonable orders of an employer that fall within the scope of the contract of employment.<sup>12</sup> In the case of *R v Darling Island Stevedoring & Lighterage Co Ltd; Ex parte Halliday*, Dixon J expressed the common law standard or test as follows:

If a command relates to the subject matter of the employment and involves no illegality, the obligation of the servant to obey it depends at common law upon its being reasonable. In other words, the lawful commands of an employer which an employee must obey are those which fall within the scope of the contract of service and are reasonable.<sup>13</sup>

13.12 How does this apply to APS employees? Section 13(5) of the *Public Service Act* expressly requires that an APS employee 'must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction'.<sup>14</sup> A supervisor has implied authority to direct subordinate staff: he or she does not require an express authorisation by the agency head to issue directions.<sup>15</sup>

13.13 The test for the lawfulness of a direction given to an APS employee is likely to be broader than the contractual formulation. The Australian Government Solicitor (AGS) has advised that:

Whilst public servants are in an employment relationship, that relationship has a constitutional and statutory setting which includes values and interests which go

8 *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 136–137.

9 Thomson Legal and Regulatory, *The Laws of Australia*, vol 26 Labour Law [26.1.131] (as at 28 May 2009). A term of mutual trust and confidence is also implied into all employment contracts: [26.1.120].

10 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, 145–146.

11 *Ibid*, 145–146.

12 *R v Darling Island Stevedoring & Lighterage Co Ltd; Ex parte Halliday* (1938) 60 CLR 601. A requirement to obey lawful and reasonable directions is implied in the contract of employment between a public servant and the Commonwealth: *Bayley v Osborne* (1984) 4 FCR 141.

13 *R v Darling Island Stevedoring & Lighterage Co Ltd; Ex parte Halliday* (1938) 60 CLR 601, 621–622.

14 *Public Service Act 1999* (Cth) s 13(5).

15 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

beyond bare matters of employment. A direction to an APS employee can be lawful if it involves no illegality and if it is reasonably adapted to protect the legitimate interests of the Commonwealth as employer or to discharge the obligations of the Commonwealth as an employer. Also, the direction must be reasonable in all the circumstances.<sup>16</sup>

### Secrecy obligations under the *Public Service Act*

13.14 The *Public Service Act* is the principal legislation regulating employment relations in the APS. Section 13 of the Act sets out the APS Code of Conduct, which binds APS employees, the secretary of a department, the head of an executive agency or statutory agency, and statutory officeholders.<sup>17</sup> The Code of Conduct requires, among other things, that an APS employee:

- comply with all applicable Australian laws, when acting in the course of APS employment, which includes secrecy laws;<sup>18</sup>
- maintain appropriate confidentiality about dealings that the employee has with any minister or minister's member of staff;<sup>19</sup> and
- comply with any other conduct requirement that is prescribed in the regulations.<sup>20</sup>

13.15 Regulation 2.1 of the *Public Service Regulations 1999* (Cth) is the only other conduct requirement currently prescribed in the regulations. The regulation is set out in full in Appendix 5. The regulation requires that:

- (3) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.
- (4) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if the information:
  - (a) was, or is to be, communicated in confidence within the government; or
  - (b) was received in confidence by the government from a person or persons outside the government;

whether or not the disclosure would found an action for breach of confidence.

<sup>16</sup> Ibid. Where a direction is incompatible with the implied constitutional freedom of political communication then it will not be 'lawful and reasonable': *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

<sup>17</sup> *Public Service Act 1999* (Cth) ss 7, 14.

<sup>18</sup> Ibid s 13(4).

<sup>19</sup> Ibid s 13(6).

<sup>20</sup> Ibid s 13(13).

13.16 Exceptions to the prohibitions on disclosure apply where:

- the information is disclosed in the course of the employee's duties;
- the information is disclosed in accordance with an authorisation given by an agency head;
- the disclosure is otherwise authorised by law; or
- the information is lawfully in the public domain.<sup>21</sup>

13.17 The regulation also expressly preserves an agency head's authority to give 'lawful and reasonable directions' regarding the disclosure of information.<sup>22</sup>

### **Role for secrecy provisions in the *Public Service Act***

13.18 Considering the confidentiality obligations imposed on employees under the general law, and the criminal secrecy offences that apply to Commonwealth officers and others, a question arises as to whether administrative secrecy provisions such as those in the APS Code of Conduct serve any additional role.

13.19 Soon after the Public Service Bill 1997 (Cth)<sup>23</sup> was introduced into Parliament, Dr Peter Shergold, the then Public Service Commissioner, expressed the view that the benefit of a Code of Conduct is that it provides

a public statement of the standards of behaviour expected of those who work in public employment ... While it is not possible to guarantee integrity by legislation, it is vital that the public knows what standards of conduct they are to expect from public servants. At the same time individual public servants themselves need to be clear on the ethical standards that are required of them.<sup>24</sup>

13.20 Shergold further commented that:

If all that was required of a Public Service Act was a legislative statement of how to select, appoint, manage and terminate employees we might as well not bother. It is not a legal necessity. The *Workplace Relations Act 1996* can suffice quite well. The sole purpose of a Public Service Act should be to protect the public interest of citizens. Only where the employment relationship is intrinsic to the articulation of the public interest should it be set out in separate legislation. That is the new, bold approach of the legislation introduced into Parliament a fortnight ago.<sup>25</sup>

---

21      *Public Service Regulations 1999* (Cth) reg 2.1(5).

22      Ibid reg 2.1(6).

23      The 1997 Bill was in essentially the same terms as the Public Service Bill 1999 (Cth), which was enacted as the *Public Service Act 1999* (Cth). For a legislative history of the *Public Service Act 1999* (Cth), see Explanatory Memorandum, Public Service Bill 1999 (Cth), [14]–[26].

24      P Shergold, 'A New Public Service Act: The End of the Westminster Tradition?' (1997) 85 *Canberra Bulletin of Public Administration* 32, 34.

25      Ibid, 33.

13.21 In the Issues Paper, *Review of Secrecy Laws* (IP 34), the ALRC asked whether there were any secrecy provisions which, if breached, should only give rise to administrative penalties.<sup>26</sup> Stakeholders suggested that administrative penalties may be preferable to criminal proceedings for relatively minor breaches,<sup>27</sup> or where the harm caused by the breach was likely to be relatively low.<sup>28</sup> Dr Ian Turnbull suggested that administrative penalties could be appropriate where no personal benefit is gained from the disclosure of information and there is no substantial loss to another person or damage to a public interest.<sup>29</sup> Liberty Victoria was of the view that administrative penalties should be used where there was no intentional or reckless behaviour.<sup>30</sup>

#### *ALRC's views*

13.22 Articulating secrecy provisions in the APS Code of Conduct provides a clear statement to APS employees and members of the public of the level of protection of Commonwealth information that can be expected from APS employees. As recognised by stakeholders, administrative secrecy obligations may be the only remedy available, or the most appropriate remedy, to address situations where there is no reasonable likelihood of harm as a result of an unauthorised disclosure or where an APS employee had no intention to cause harm.

13.23 By addressing the distinct context of obligations associated with employment in the public sector, administrative secrecy provisions may also protect different interests from those recognised in the criminal context. In the following sections of this chapter, the secrecy provisions in the APS Code of Conduct will be assessed in light of their capacity to satisfy the objects in the *Public Service Act* of establishing ‘an apolitical public service that is efficient and effective in serving the Government, the Parliament and the Australian public’.<sup>31</sup>

#### **Relationship between secrecy obligations and other APS requirements**

13.24 As the Australian Government Attorney-General’s Department (AGD) commented in its submission on IP 34, requirements in the *Public Service Act* other than express secrecy provisions may constrain the manner in which an APS employee communicates official information. For example, the APS Code of Conduct requires APS employees to exercise discretion when commenting on government policy in

---

26 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–13.

27 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

28 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

29 I Turnbull, *Submission SR 15*, 17 February 2009.

30 Liberty Victoria, *Submission SR 19*, 18 February 2009. The Australian Securities and Investment Commission (ASIC) submitted that administrative penalties would be appropriate where an unauthorised disclosure is inadvertent: Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

31 *Public Service Act 1999* (Cth) s 3.

order not to infringe the value of an apolitical public service.<sup>32</sup> The Code of Conduct also requires that an APS employee:

- does not make improper use of inside information, or his or her duties, status, power or authority, in order to gain a benefit or advantage for the employee or for any other person;<sup>33</sup> and
- behaves at all times in a way that upholds the integrity and good reputation of the APS.<sup>34</sup>

13.25 In their submissions on IP 34, the Australian Press Council and Australia's Right to Know (ARTK) coalition both suggested that legislation that permits government information to be kept secret or confidential should include a provision making it an offence to withhold information from the public for an improper purpose; for example, concealing corruption or maladministration.<sup>35</sup> New requirements for the disclosure of information are outside the scope of this Inquiry: these are matters for consideration in the context of freedom of information (FOI) laws. What the media submissions highlight, however, is the necessary balance between obligations of disclosure and secrecy provisions in the information-handling framework for APS employees.<sup>36</sup>

13.26 In Chapter 15, the ALRC discusses the information-handling policies of Australian Government agencies. The requirements in these policies for the disclosure of Commonwealth information will sometimes incorporate objectives beyond secrecy alone. These may include, for example, safeguards to ensure that the agency provides information that is accurate and not misleading, and that the agency is—and is seen to be—apolitical. Information-handling policies also may include requirements for employees to release information in certain circumstances.<sup>37</sup>

## **Prejudice to the effective working of government**

### **Background**

13.27 As noted above, reg 2.1(3) of the *Public Service Regulations* prohibits an APS employee from disclosing information obtained or generated in connection with that person's employment

---

32 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

33 *Public Service Act 1999* (Cth) s 13(10).

34 *Ibid* s 13(11).

35 Australia's Right to Know, *Submission SR 35*, 6 March 2009; Australian Press Council, *Submission SR 16*, 18 February 2009.

36 Protecting Commonwealth officers, including APS employees, who disclose corruption or maladministration may arise as an aspect of whistleblower protection, which is considered throughout this Discussion Paper.

37 See also Ch 4, which considers the relationship between secrecy laws and other information-handling regimes, such as FOI laws and archives.

---

if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.<sup>38</sup>

13.28 This requirement was introduced in 2006, following the decision of Finn J in *Bennett*<sup>39</sup> that its more expansive predecessor was inconsistent with the implied constitutional guarantee of freedom of communication about government and political matters.<sup>40</sup>

13.29 The Explanatory Statement for the replacement regulation describes its scope as follows:

Depending on the circumstances, this restriction could cover information such as opinions, consultation, negotiations (including about the management of a contract), incomplete research, or advice or recommendations to the Government, leading or related to, the development or implementation of the Government's policies or programs. The legitimate interest of government in regulating access to such classes of information is recognised in the *Freedom of Information Act 1982*.<sup>41</sup>

13.30 The width of the regulation has been further clarified by the Australian Public Service Commission (APSC) in its *APS Values and Code of Conduct in Practice*:

APS employees need to consider on each occasion whether the disclosure of information could damage the effective working of government, including, for example, in relation to unclassified information and in circumstances where there is no relevant Agency Head direction ...

The exemptions set out in the FOI Act are a useful starting point in determining which categories of information may potentially fall within the scope of regulation 2.1.<sup>42</sup>

13.31 Several other jurisdictions have also linked a public servant's obligation of non-disclosure to potential prejudice to the role or functions of government. For example, s 57 of the *Public Sector Management Act 1995* (SA) sets out a general prohibition on the disclosure of official information by South Australian government employees, except to the extent that the disclosure is authorised under the regulations. One such exception applies where the disclosure or comment:

- (i) does not give rise to any reasonably foreseeable possibility of prejudice to the Government in the conduct of its policies, having regard to the nature of the disclosure or comment, the employee's current position or previous positions in

---

38 *Public Service Regulations 1999* (Cth) reg 2.1(3).

39 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334. *Bennett* is considered further in Chs 2–3.

40 The now repealed and replaced reg 7(13) of the *Public Service Regulations 1935* (Cth) provided that: 'An APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head's express authority, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge'.

41 Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006).

42 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 23 September 2008.

the Public Service and the circumstances in which the disclosure or comment is made; and

- (ii) is not made with a view to securing a pecuniary or other advantage for the employee or any other person; and
- (iii) does not involve—
  - (A) any disclosure of information contrary to any law or lawful instruction or direction; or
  - (B) any disclosure of trade secrets or information of commercial value the disclosure of which would diminish its value or unfairly advantage a person in commercial dealings with the Government; or
  - (C) any disclosure of information in breach of intellectual property rights.<sup>43</sup>

13.32 Another example is found in one of the standards of conduct that the *UK Civil Service Management Code* requires departments and agencies to include in staff regulations, namely that

civil servants must not seek to frustrate the policies or decisions of Ministers by the use or disclosure outside the Government of any information to which they have had access as civil servants.<sup>44</sup>

13.33 A key consideration in assessing whether there is a need to reform the prohibition on an APS employee disclosing information that could ‘prejudice the effective working of government’ is whether or not the prohibition is consistent with the implied constitutional guarantee of freedom of communication about government and political matters.

13.34 As discussed in detail in Chapter 2, in *Bennett*,<sup>45</sup> Finn J found that the predecessor to reg 2.1 impaired the implied freedom of political communication in an unnecessary and unreasonable way. On that basis, it was inconsistent with the *Australian Constitution* and invalid. The amended regulation, however, was upheld by Refshauge J, of the ACT Supreme Court, in *R v Goreng Goreng* (*'Goreng Goreng'*).<sup>46</sup> Refshauge J expressed the view that the regulation was not a ‘catch-all’ provision like its predecessor, but rather a more focused and targeted provision that sought to protect a legitimate government interest.<sup>47</sup>

---

<sup>43</sup> *Public Sector Management Regulations 1995* (SA) reg 15(d).

<sup>44</sup> Minister for the Civil Service (UK), *Civil Service Management Code* <[www.civilservice.gov.uk/iam/codes/csmc/index.asp](http://www.civilservice.gov.uk/iam/codes/csmc/index.asp)> at 17 September 2008.

<sup>45</sup> *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

<sup>46</sup> *R v Goreng Goreng* [2008] ACTSC 74.

<sup>47</sup> *Ibid*, [37].

## Submissions and consultations

13.35 In IP 34, the ALRC asked whether reg 2.1 of the *Public Service Regulations* provides an appropriate model for protecting Commonwealth information in a way that is consistent with the implied constitutional freedom of political communication.<sup>48</sup>

13.36 The AGD noted that the constitutionality of the provision had been upheld by the ACT Supreme Court and suggested that the regulation may be a useful guide for some other secrecy laws.<sup>49</sup> The AGD supported reg 2.1 as ‘an example of a general secrecy law designed to protect sensitive government information that is reasonably likely to cause some identifiable harm’.<sup>50</sup>

13.37 Other stakeholders, however, raised concerns about the potential width of the provision. The ARTK coalition commented that phrases such as the ‘effective working of government’ are overly broad and subjective and that there is potential for the phrase to be construed so broadly that it could encompass almost any administrative or governmental activity.<sup>51</sup>

13.38 The Community and Public Sector Union (CPSU) submitted that reg 2.1 ‘does not adequately prescribe the employment related nature of the duties regarding disclosure of information, nor provide adequate defences for disclosure’.<sup>52</sup> The Public Interest Advocacy Centre (PIAC) expressed the view that prohibiting the disclosure of information that could prejudice the ‘effective’ working of government is far too broad:

Understood at its simplest, an action is *effective* if it brings about an expected result. Expressed at such a high level of generality, the interest sought to be protected (‘the *effective* workings of government’) may frequently be in tension with other important public interests, such as the *transparent* workings of government.<sup>53</sup>

13.39 PIAC was also concerned that reg 2.1 does not give any guidance about the *degree* of prejudice required, or require that countervailing public interests favouring disclosure be taken into account.<sup>54</sup>

---

48 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–8.

49 Attorney-General’s Department, *Submission SR 36*, 6 March 2009. Circumstances where the Department did not consider reg 2.1 to be an appropriate model were offences that needed to be tailored to specific regulatory or agency requirements. This issue is discussed in Ch 2.

50 Ibid.

51 Australia’s Right to Know, *Submission SR 35*, 6 March 2009. See also: R Fraser, *Submission SR 42*, 23 March 2009.

52 Community and Public Sector Union, *Submission SR 32*, 2 March 2009. The CPSU was also concerned about the current connection between reg 2.1 and s 70 of the *Crimes Act 1914* (Cth). See also N Rogers, *Submission SR 01*, 9 December 2008, who answered this question in the negative.

53 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

54 Ibid. PIAC also suggested that the secrecy provisions in ss 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth) could be inconsistent with the implied constitutional freedom of political communication.

13.40 Whistleblowers Australia submitted that the regulation was ‘almost puerile’, as ‘it neither ensures ready access to information nor does it provide security where it is needed’. The organisation questioned whether employees would be able to foresee the likely impact of a disclosure on the effective working of government. Would this depend, for example, on whether a leaked policy document was accepted or rejected by the Australian public?

The regulation is so imprecise and unclear as to dissuade any reasonably cautious employee from making any comments about the public sector. It unnecessarily burdens the employee, because it lacks precision and does not afford clear advice about what may or may not be disclosed. The purpose of the regulation appears to be to maintain control over public interest disclosures, and that cannot be an appropriate constitutional purpose adapted for a legitimate end.<sup>55</sup>

13.41 Ron Fraser commented that, although reg 2.1 ‘had survived one constitutional challenge, and may continue to do so’, the scope of the provision is still ‘very wide and relatively unspecific’.<sup>56</sup> Fraser questioned whether reg 2.1 should be reframed to include an element of actual or intended damage, and remodelled to incorporate some or all of the elements of the common law duty of good faith and fidelity.<sup>57</sup>

13.42 The Australian Intelligence Community (AIC) advised that reg 2.1 was not an appropriate model to protect national security-classified information.<sup>58</sup>

### **Options for reform**

13.43 The principal concern that stakeholders raised about reg 2.1 is its uncertain scope. These submissions mirror reservations that Refshauge J expressed in the *Goreng Goreng* case, where it was with ‘considerable hesitation’ that he upheld reg 2.1 as meeting the requisite standard of certainty, on the basis ‘that public servants will, by and large, comprehend what is encompassed’.<sup>59</sup>

13.44 One option for reducing the current uncertainty about the scope of reg 2.1 is to amend the provision to reflect more closely the conduct requirements found in other secrecy provisions. Two aspects of the regulation appear to be particularly broad—the application to information that an APS employee obtains or generates ‘in connection with’ his or her employment; and the requirement that the disclosure ‘could be prejudicial’ to the effective working of government.

---

55 Whistleblowers Australia, *Submission SR 40*, 10 March 2009. Whistleblowers Australia also raised concerns about the use of ‘lawful and reasonable directions’ by an agency.

56 R Fraser, *Submission SR 42*, 23 March 2009. Accordingly, Mr Fraser submitted that the provision was more appropriate for administrative measures than criminal penalties, as is currently the situation as a result of s 70 of the *Crimes Act 1914* (Cth).

57 R Fraser, *Submission SR 42*, 23 March 2009.

58 Australian Intelligence Community, *Submission SR 37*, 6 March 2009. No rationale was provided for this view.

59 *R v Goreng Goreng* [2008] ACTSC 74, [55].

13.45 Contention also surrounds the subjective nature of the determination of whether a particular disclosure would cause harm to ‘the effective working of government’. A clearer and more targeted definition of harm could be developed by linking APS employees’ obligations of non-disclosure to other information-management regimes in the APS such as the *Freedom of Information Act 1982* (Cth) (FOI Act).

13.46 Each of these options for reform are considered below.

***In connection with***

13.47 Secrecy provisions commonly include a requirement that there be a particular connection between the information that is the subject of protection and the manner in which the information came into the possession of a regulated party.<sup>60</sup> The most frequently used formulation is that the regulated party has acquired the information ‘in the course of’, or ‘in the performance of’, his or her functions or duties.<sup>61</sup> Other secrecy provisions are framed causatively—that is, that the regulated party has acquired the information ‘because of’, or ‘by reason of’, his or her official position.<sup>62</sup>

13.48 The obligations of reg 2.1 apply to information that an APS employee obtains or generates ‘in connection with’ his or her employment. This is an unusual formulation. The ALRC has identified only 10 other secrecy provisions that use the phrase ‘in connection with’ to limit the scope of information protected. The majority of these are information-handling rules for Australian Government agencies and other legal entities,<sup>63</sup> as compared with obligations of non-disclosure that apply to individuals.<sup>64</sup>

13.49 The scope of information acquired ‘in connection with’ an officer’s functions or duties has not been judicially considered in the context of reg 2.1 or other secrecy provisions. Some limited guidance, however, may be drawn from the interpretation of this phrase in other legislation. In adjudicating on the exemption from the requirement to provide a statement of reasons for decisions under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) for decisions ‘in connection with’ a criminal offence, Davies J noted that:

---

60 In its mapping exercise, the ALRC identified more than 130 secrecy provisions that include a requirement for a particular nexus between the information protected and the party regulated.

61 The ALRC has identified this formulation in approximately 25% of all secrecy provisions that specify the requisite connection between the party regulated and the information protected. See, eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 65; *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30; *Australian Federal Police Act 1979* (Cth) s 60A; *Excise Act 1901* (Cth) s 159.

62 See, eg, *Gene Technology Act 2000* (Cth) s 187; *Australian Hearing Services Act 1991* (Cth) s 67; *Export Finance and Insurance Corporation Act 1991* (Cth) s 87; *Sex Discrimination Act 1984* (Cth) s 112.

63 *Water Act 2007* (Cth) s 215; *Australian Securities and Investments Commission Act 2001* (Cth) ss 127(1), (4EA), 213; *Bankruptcy Regulations 1996* (Cth) regs 8.05O, 8.32; *Trade Practices Act 1974* (Cth) s 44AAF.

64 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S; *National Water Commission Act 2004* (Cth) s 43; *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63.

Expressions such as ‘relating to’, ‘in relation to’, ‘in connection with’ and ‘in respect of’ are commonly found in legislation but invariably raise problems of statutory interpretation. They are terms which fluctuate in operation from statute to statute ... The terms may have a very wide operation but they do not usually carry the widest possible ambit, for they are subject to the context in which they are used, to the words with which they are associated and to the object or purpose of the statutory provision in which they appear.<sup>65</sup>

13.50 Whether or not an act is done in connection with a person’s employment has been considered in the context of s 106 of the *Sex Discrimination Act 1984* (Cth) (SDA), which makes an employer liable for certain acts done by an employee ‘in connection with the employment of the employee’. In the case of *South Pacific Resort Hotels Pty Ltd v Trainor*, for example, the Federal Court accepted that sexual harassment by a fellow employee that occurred while both were off-duty and while they were not performing any function related to their employment nonetheless fell within the scope of the provision.<sup>66</sup> A sufficient nexus arose out of the fact that the incident occurred on the employer’s land and in a building in which some (but not all) staff resided. Black CJ and Tamberlin J noted that:

it could not be said here that the common employment was unrelated or merely incidental to the sexual harassment of one by the other.

The expression ‘in connection with’ in its context in s 106(1) of the SDA is a broad one of practical application and ... the facts here point readily to the conclusion that Mr Anderson’s conduct in the staff accommodation was ‘in connection with’ his employment within the meaning of s 106(1) of the SDA ...

We would add that the expression chosen by the Parliament ... would seem, on its face, to be somewhat wider than the familiar expression ‘in the course of’ used with reference to employment in cases about vicarious liability at common law or in the distinctive context of workers compensation statutes.<sup>67</sup>

#### ***Reasonably foreseeable that the disclosure could be prejudicial***

13.51 The secrecy obligations in reg 2.1 apply ‘if it is reasonably foreseeable that the disclosure *could be* prejudicial to the effective working of government’.<sup>68</sup> This sets out an objective test, based on what a reasonable person would decide in the same circumstances and with the same information.<sup>69</sup> In a motion for disallowance of the *Public Service Amendment Regulations 2004* (Cth)—which included an identical provision to the current reg 2.1—Senator Kim Carr commented that:

‘could be prejudicial’ is ... an extremely broad definition of an action and one which I say is aimed at intimidating public servants into not speaking out on any matter,

---

65     *Hatfield v Health Insurance Commission* (1987) 15 FCR 487, 491.

66     *South Pacific Resort Hotels Pty Ltd v Trainor* (2005) 144 FCR 402.

67     Ibid, 409–410.

68     *Public Service Regulations 1999* (Cth) reg 2.1 (emphasis added).

69     Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006), 2.

because any action ‘could be prejudicial’ if the political masters of the Public Service deem it to be so.<sup>70</sup>

13.52 The operation of a small number of secrecy provisions depends on the disclosure of information resulting in an identified consequence. For example, various secrecy provisions in the *Migration Act 1958* (Cth) prohibit disclosure of the name of a non-citizen or ‘any information that *may* identify the non-citizen’.<sup>71</sup> The *Proceeds of Crime Act 2002* (Cth) prohibits the disclosure of ‘information from which another person *could* infer the existence or nature of a production order’.<sup>72</sup> A higher threshold is set by several provisions that require that the disclosure of information would be ‘likely’ to lead to identification of a person.<sup>73</sup> The *Auditor-General Act 1997* (Cth) requires an even greater degree of certainty—that information must not be included in public reports that ‘would’ be contrary to the public interest.<sup>74</sup>

### ***Effective working of government***

13.53 In submissions on IP 34, many stakeholders raised concerns about the subjective and imprecise nature of the formula of harm to ‘the effective working of government’ where it stands alone. Other laws and practices that characterise the sensitivity of Commonwealth information could be used to provide clearer guidance to APS employees and agencies about the application of the regulation. These include the FOI Act and security classifications.

### ***FOI Act***

13.54 The FOI Act provides members of the public with a general right of access to documents held by Australian Government agencies and ministers unless an exemption applies.<sup>75</sup> As discussed in Chapter 4, exempt documents under the FOI Act include, for example, documents:

- where disclosure could damage identified interests of the Australian Government, such as security, defence or international relations, relations with a state or territory, law enforcement operations and public safety or the life or physical safety of any person; and
- that involve a particular class of information, such as information communicated in confidence to the Australian Government by or on behalf of another government, Cabinet or Executive Council documents, information subject to

70 Commonwealth, *Parliamentary Debates*, Senate, 16 June 2005, 38 (K Carr), 41.

71 *Migration Act 1958* (Cth) ss 46A, 46B, 48B, 72, 91F, 91L, 91Q (emphasis added).

72 *Proceeds of Crime Act 2002* (Cth) s 210 (emphasis added). See also: *Australian Crime Commission Act 2002* (Cth) s 9; *Ombudsman Act 1976* (Cth) s 35B.

73 *Referendum (Machinery Provisions) Act 1984* (Cth) s 116; *Banking Act 1959* (Cth) s 52E, *Commonwealth Electoral Act 1918* (Cth) s 323.

74 *Auditor-General Act 1997* (Cth) s 37.

75 The *Freedom of Information Act 1982* (Cth) is discussed in Ch 4. See also Ch 2 in relation to the FOI Act as an expression of ‘open government’ principles.

certain specified secrecy provisions, internal working documents and trade secrets or other commercial information.<sup>76</sup>

13.55 Exemptions also apply to documents that have originated with, or been received from, certain agencies—principally agencies of the Australian Intelligence Community.<sup>77</sup>

13.56 A number of submissions in response to IP 34 suggested that the secrecy obligations of Commonwealth officers should be more closely aligned with the FOI Act. As noted by the Treasury:

The purposes of the FOI law and taxation secrecy provisions are broadly consistent. One is designed to promote access to records to support a desire of open and transparent government and the other is to give effect to the legitimate expectations of taxpayers that their sensitive information will be treated appropriately. Given the consistency in purpose, the issue becomes how they can be reconciled legislatively.<sup>78</sup>

13.57 A similar point was made by the Department of Human Services (DHS), which suggested that the basis for exempting information from disclosure under the FOI Act could also provide the basis for the scope of the information required to be protected by secrecy provisions. The DHS submitted that:

where secrecy provisions cover information which is innocuous and its disclosure would cause no harm, there would seem to be no justification for a provision prohibiting its disclosure.<sup>79</sup>

13.58 The CPSU suggested that any changes to secrecy provisions to clarify their scope or application should be tailored to fit with the principles of open and transparent government and legislation dealing with FOI and privacy. Secrecy provisions and public access to information should not be viewed as opposed to one another, but complementary.<sup>80</sup> The ARTK coalition also supported a coherent approach to secrecy provisions and other legislation, such as FOI.<sup>81</sup>

### ***Security classification***

13.59 Another practice governing the handling of Commonwealth information is the security classification system set out in the *Australian Government Protective Security Manual* (PSM).<sup>82</sup> As discussed in Chapter 3, an agency's decision to give information a security classification is based on a determination of the damage that could be caused

76 Ibid ss 33–47A.

77 Ibid s 7.

78 The Treasury, *Submission SR 22*, 19 February 2009. See also Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

79 Department of Human Services, *Submission SR 26*, 20 February 2009.

80 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

81 Australia's Right to Know, *Submission SR 35*, 6 March 2009.

82 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual (PSM)* (2005).

to national security (in the case of national security information) or other interests (in the case of non-national security information) if the information were to be compromised. The PSM sets out minimum procedural requirements for the use, storage, transmission and disposal of security classified information.<sup>83</sup>

13.60 In its submission, the AIC expressed the view that ‘national security-classified information should be treated as a specific category of information for the purposes of secrecy provisions’.<sup>84</sup> The CPSU also linked its discussion to the security classification system, submitting that:

legislative secrecy provisions should not apply generally to all Commonwealth information, but should distinguish between classified or secret information and other types of information which may nonetheless still be not publicly available.<sup>85</sup>

13.61 As noted in Chapter 3, in its discussion of the appropriate relationship between secrecy laws and the FOI Act, Liberty Victoria suggested that a ‘more consistent and principled approach’ to the disclosure of information would be to replace the existing FOI exemptions with an exemption provision based on the classification system in the PSM. Under the organisation’s proposed system, all non-classified information would, *prima facie*, be subject to production.<sup>86</sup>

### ALRC’s views

13.62 For the APS to serve the needs of the Australian Government, the Parliament and the Australian public, in accordance with the objects of the *Public Service Act*, there must be confidence that APS employees will not disclose information in potentially harmful circumstances. Agencies rely on employees complying with internal processes for the release of official information to ensure that only material that is accurate and properly reflective of the views of the Australian Government is issued in their name. Ministers and others seeking to engage in sensitive policy discussions with the APS must trust that these deliberations will be treated confidentially. Members of the public also expect the APS to accord information that they provide to it with a high level of respect. Important aspects of government administration, such as the taxation and welfare systems, rely on citizens making full disclosure of sensitive personal and financial information, trusting that such information will not be disclosed publicly.

13.63 In the ALRC’s view, a provision in the Code of Conduct prohibiting the disclosure of information harmful to the ‘effective working of government’—as set out in reg 2.1 of the *Public Service Regulations*—is an appropriate mechanism to accommodate the broad-ranging situations that may warrant disciplinary action. Defining the harm more narrowly risks omitting situations that could legitimately be

---

83 Ibid.

84 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

85 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

86 Liberty Victoria, *Submission SR 19*, 18 February 2009.

the subject of disciplinary proceedings. However, valid concerns have been raised that APS employees have insufficient guidance on what disclosures will be—or might be—encompassed by the regulation.

13.64 These concerns may be reduced by making some minor reforms to the application of the regulation. First, the scope of the conduct regulated can be narrowed to reflect more closely other secrecy provisions. Secondly, a framework can be developed for interpreting when a disclosure will cause harm to the effective working of government. These options for reform are explained more fully below.

#### ***Narrowing the scope of conduct regulated***

13.65 Regulation 2.1 protects information from disclosure in a broader set of circumstances than many other secrecy provisions. In particular, the regulation covers:

- information that an APS employee obtains or generates ‘in connection with’ his or her employment; and
- disclosures where it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government.

13.66 In relation to the first element, reg 2.1 could apply where an APS employee obtains information in a situation considerably divorced from his or her actual duties of employment. For example, an APS employee may be introduced to a person as a result of his or her APS employment and develop a personal friendship. If that person later gives the APS employee information in his or her personal capacity, and the APS employee further discloses this information (again in his or her personal capacity), it is possible that the information could have been received by the APS employee ‘in connection with’ his or her employment. This scenario is unlikely to satisfy narrower formulations in other secrecy provisions, which require, for example, that the information was received ‘in the course of’ the APS employee’s employment.

13.67 In Chapter 8, the ALRC expresses the view that the proposed new general secrecy offence should apply to ‘any information to which a person has, or had access, by reason of his or her being, or having been, a Commonwealth officer’.<sup>87</sup> An equivalent formulation would appear advantageous for a revised reg 2.1.<sup>88</sup> In particular, this ensures that the administrative secrecy provision only extends to situations where there is a causal connection between the information that is the subject of disclosure and an APS employee’s employment. Where an APS employee has obtained Commonwealth information outside his or her public employment, then the ALRC considers that normally he or she should be able to participate freely in discussion and debate on the information.

---

87      Proposal 8–5.

88      Proposal 13–1.

13.68 As noted above, reg 2.1 also applies to disclosures where it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government. This threshold may be too low. Given the inherent uncertainty in determining whether or not a particular disclosure would result in such harm, a rigorous threshold is important to forestall the potentially indiscriminate application of the provision. At this stage, the ALRC considers the appropriate threshold to be where the disclosure is ‘reasonably likely’ to be prejudicial to the effective working of government.<sup>89</sup> This formulation balances the difficulty for a disciplinary authority of proving that a disclosure would, in fact, harm the effective working of government, with the need to set a threshold high enough to avoid the provision being used as a catch-all. A requirement of a ‘reasonable likelihood’ of harm is also consistent with the threshold that the ALRC has set out in the proposed general secrecy offence.<sup>90</sup>

### ***Developing an interpretive framework***

13.69 The ALRC reaches the preliminary view, as noted above, that ‘harm to the effective working of government’ remains suitable as the overarching element for the administrative secrecy obligations of APS employees. However, other laws and practices that govern the flow of Commonwealth information could play a useful role in interpreting whether information disclosed by an APS employee is of such a nature as to harm the effective working of government.

13.70 As noted in Chapter 4, s 3(1)(b) of the FOI Act provides that the objects of the Act include the creation of a general right of access to Commonwealth information, limited only to the extent

necessary for the protection of essential public interests and the private and business affairs of persons in respect of whom information is collected and held by departments and public authorities.<sup>91</sup>

13.71 The FOI Act sets out a range of circumstances in which an Australian Government agency can deny a request for access to Commonwealth documents. In developing these FOI exemptions, the Australian Parliament has indicated the types of information that warrant a heightened level of protection. The ALRC has formed the preliminary view that the FOI exemptions can be relied on as indicative of the circumstances in which disclosure has the potential to prejudice the effective working of government. Both the Explanatory Statement for reg 2.1 and the *APS Values and Code of Conduct in Practice* also support the use of the FOI framework as a guide for assessing whether the disclosure of information harms the effective working of government. This also facilitates a complementary approach to secrecy and FOI in an agency’s information-handling regime.

<sup>89</sup> Proposal 13–1.

<sup>90</sup> Proposal 7–1.

<sup>91</sup> The objects clause in the Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft focuses on providing members of the public with access to government information, without further reference to the exemptions from this right of access. See Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 1.

13.72 Under s 14 of the FOI Act, Australian Government agencies are encouraged to make information available outside the FOI regime. The exposure draft of the Freedom of Information Amendment (Reform) Bill 2009 (Cth) further emphasises the informal release of information by extending the current protections against civil and criminal liability for the provision of information under the FOI Act to agencies and officers that publish information other than under the FOI Act.<sup>92</sup> Accordingly, the ALRC proposes that, in interpreting whether or not the disclosure of certain information would be reasonably likely to harm the effective working of government, disciplinary authorities should consider the likelihood of that information being released under the FOI Act or through some other means.<sup>93</sup>

13.73 The ALRC has not included the security classification of a document under the PSM as an express consideration for interpreting the likelihood of harm based on the nature of information that has been disclosed by an APS employee. This is consistent with the ALRC's focus on assessing the consequences of the disclosure of information on a case-by-case basis, rather than relying on a proxy status such as its classification level. Where Commonwealth information has been mis-classified, or over-classified, for example, its security classification may not be a good indication of the harm that disclosure of the information is likely to cause.

13.74 The security classification of a document, however, could point towards the likelihood that the *circumstances* of disclosure could harm the effective working of government. The nature of information is not usually sufficient, in and of itself, to determine the likelihood of harm to the effective working of government resulting from unauthorised disclosure by an APS employee. In some situations, this harm will result, not from the sensitive nature of the information, but because of the circumstances of disclosure. For example, a senior APS employee could give a 'tip off' to a journalist that he or she should lodge an FOI request with regard to certain documents because exposure would be likely to cause public embarrassment to the Australian Government. Or an APS employee could consistently fail to follow an agency's policy for the release of information, leading to the disclosure of inaccurate or superseded material. In both of these situations, the circumstances surrounding the disclosure may breach the necessary trust and confidence between employer and employee even though the actual information disclosed is unlikely to cause harm in and of itself.<sup>94</sup>

13.75 In order to determine whether or not the circumstances of a disclosure of information by an APS employee are reasonably likely to harm the effective working of government, a disciplinary authority should consider whether or not the employee has taken reasonable steps to comply with the agency's information-handling policy or another lawful and reasonable direction regarding the disclosure of information. This

92 The protections against civil and criminal liability are set out in ss 91 and 92 of the *Freedom of Information Act 1982* (Cth). Proposed extensions to this framework are set out in sch 6 of the Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft.

93 Proposal 13–2.

94 See previous discussion of the duty of fidelity and loyalty.

test would encompass both an APS employee who intentionally breaches the policies and processes in place for information handling, as well as an employee who performs his or her information-handling responsibilities without due care and diligence.

#### *Applying the interpretive framework*

13.76 The respective importance of the factors identified above will differ on a case-by-case basis. Where, for example, the information disclosed is of a particularly sensitive nature, the disclosure could harm the effective working of government even where the circumstances of disclosure evidence little or no moral culpability on the part of the APS employee. Similarly, the more reprehensible the conduct of the APS employee, the less sensitive the information may need to be before a disciplinary authority is satisfied that the disclosure was reasonably likely to cause the requisite harm.

13.77 Although the ALRC considers that the nature of the information disclosed and the circumstances of disclosure will be the most common indicia of the likelihood of the requisite harm, situations may arise where other factors are relevant. To accommodate this possibility, the ALRC's proposal for an interpretive framework is framed non-exhaustively.

**Proposal 13–1** Regulation 2.1 of the *Public Service Regulations 1999* (Cth) should be amended to apply to information:

- (a) to which an Australian Public Service employee has access by reason of his or her employment; and
- (b) where the disclosure is reasonably likely to prejudice the effective working of government.

**Proposal 13–2** Regulation 2.1 of the *Public Service Regulations 1999* (Cth) should specify that, in determining whether a disclosure of information is reasonably likely to prejudice the effective working of government, the disciplinary authority should have regard to factors such as:

- (a) the nature of the information disclosed, including the likelihood that it would be subject to release under the *Freedom of Information Act 1982* (Cth) or through some other means; and
- (b) the circumstances in which the disclosure is made, including whether the Australian Public Service employee took reasonable steps to comply with the agency's information-handling policy or any lawful and reasonable direction concerning the disclosure of information.

## **Information communicated in confidence**

### **Background**

13.78 As set out above, reg 2.1(4) of the *Public Service Regulations* prohibits an APS employee from disclosing information which the employee has obtained or generated in connection with his or her employment if the information:

- (a) was, or is to be, communicated in confidence within the government; or
- (b) was received in confidence by the government from a person or persons outside the government;

whether or not the disclosure would found an action for breach of confidence.<sup>95</sup>

13.79 The Explanatory Statement for the revised regulation advises that:

Information will be taken to be received in confidence by the government from a person or persons outside the government where the provision of the information is subject to an express confidentiality condition (whether in a contract or otherwise), and in other circumstances where it is clear that the information is provided on the basis that it is to be used only for the purpose for which it is provided. Again, the nature and context of the information may make it clear that the information is disclosed on a confidential basis (eg information provided by a foreign State about its likely position in a treaty negotiation or information provided by a commercial entity which would be useful to its competitors).<sup>96</sup>

13.80 The Explanatory Statement notes that other circumstances that may indicate that the information has been given in confidence include where information is given to an employee on the understanding that it is only to be disclosed in the course of official duties—for example, where the information has been given a security classification.<sup>97</sup>

### **Duplicating ‘harm to the effective working of government’?**

13.81 In Proposal 13–2, the ALRC formulates a test for assessing the harm to the effective working of government that could result from the disclosure of Commonwealth information for the purpose of reg 2.1(3). This involves interpreting harm both as a function of the nature of the information disclosed and the circumstances of disclosure. An indication that harm could result from the nature of the information is that the information would not be subject to release under the FOI Act or otherwise.

13.82 Given this proposal, is there a need for an additional secrecy provision for the specific instance of information communicated in confidence? A number of exemptions in the FOI Act protect confidential information held by the Australian Government from access in certain circumstances. First, a document may be classified

---

95     *Public Service Regulations 1999* (Cth) reg 2.1(4).

96     Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006), 3.

97     Ibid.

as an exempt document under the FOI Act ‘if its disclosure under this Act would found an action, by a person (other than an agency or the Commonwealth), for breach of confidence’.<sup>98</sup>

13.83 As discussed in Chapter 5, the equitable action for breach of confidence applies to ‘confidential information improperly or surreptitiously obtained or of information imparted in confidence which ought not to be divulged’.<sup>99</sup> In *Commonwealth v Fairfax*, the High Court accepted that—although the equitable action was developed to protect the personal, private and proprietary interests of the citizen—the principles could be applied to protect information in the hands of government. To do so, not only must the confidential nature of the information be shown, but also that an unauthorised use of that information would be to the detriment of the party communicating it.<sup>100</sup> Significantly, the decision noted that mere exposure of the government to public discussion and criticism will not constitute a relevant detriment. Rather,

the court will determine the government’s claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.<sup>101</sup>

13.84 Documents also may be exempt documents under the FOI Act if disclosure

would divulge any information or matter communicated in confidence by or on behalf of a foreign government, an authority of a foreign government or an international organization to the Government of the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth or of an authority of the Commonwealth.<sup>102</sup>

### ALRC’s views

13.85 There is substantial overlap between reg 2.1(4)—information communicated in confidence—and the ALRC’s proposed revised reg 2.1(3)—information which, if disclosed, would be ‘reasonably likely to be prejudicial to the effective working of government’. To the extent that the prohibition on the disclosure of information communicated in confidence applies beyond the limits of reg 2.1(3)—for example, where the disclosure of Commonwealth information received in confidence is unlikely to injure the public interest—the ALRC is not convinced that there is a valid public policy basis for exposing an APS employee to disciplinary action.

98 *Freedom of Information Act 1982* (Cth) s 45. The exemption does not apply to certain official documents unless the disclosure would constitute a breach of confidence owed to a person or body other than: a minister or ministerial officer or an Australian Government agency or officer of an agency. The Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft does not amend this exemption.

99 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50, citing Swinfen Eady LJ in *Lord Ashburton v Pope* (1913) 2 Ch 469, 475.

100 *Commonwealth v Fairfax* (1980) 147 CLR 39, 51.

101 *Ibid*, 52.

102 *Freedom of Information Act 1982* (Cth) s 33(b). An equivalent exemption applies to information or matter communicated in confidence by or on behalf of a state: s 33A. The Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft does not amend these exemptions.

13.86 Consequently, in the ALRC's preliminary view, the prohibition on the disclosure of confidential information set out in reg 2.1(4) of the *Public Service Regulations* is unnecessary and should be removed. As this issue was not expressly canvassed in IP 34, the ALRC is particularly interested in hearing from stakeholders whether there is information protected by the provision that would not otherwise be covered through reg 2.1(3), disclosure of which should warrant disciplinary action.

13.87 The above analysis has focused on situations where the nature of the information disclosed by an APS employee warrants disciplinary action under reg 2.1(3). It is also important to note that sometimes disciplinary action could be justified on the basis of the circumstances surrounding the disclosure of information communicated in confidence: for example, an employee who fails to take reasonable steps to comply with the requirements of the PSM for dealing with security classified information.

**Proposal 13–3** The express prohibition on the disclosure of information communicated in confidence set out in reg 2.1(4) of the *Public Service Regulations 1999* (Cth) should be removed.

## Exceptions and defences

### Background

13.88 The prohibitions set out in regs 2.1(3) and (4) of the *Public Service Regulations* do not prevent an APS employee from disclosing information if:

- (a) the information is disclosed in the course of the APS employee's duties; or
- (b) the information is disclosed in accordance with an authorisation given by an Agency Head; or
- (c) the disclosure is otherwise authorised by law; or
- (d) the information that is disclosed:
  - (i) is already in the public domain as the result of a disclosure of information that is lawful under these Regulations or another law; and
  - (ii) can be disclosed without disclosing, expressly or by implication, other information to which subregulation (3) or (4) applies.<sup>103</sup>

13.89 The *Public Service Regulations* do not include an express exception or defence for public interest disclosures by APS employees. Some protection, however, is provided by s 16 of the *Public Service Act*, which states that:

---

103 *Public Service Regulations 1999* (Cth) reg 2.1(5).

A person performing functions in or for an Agency must not victimise, or discriminate against, an APS employee because the APS employee has reported breaches (or alleged breaches) of the Code of Conduct to:

- (a) the [Public Service] Commissioner or a person authorised for the purposes of this section by the Commissioner; or
- (b) the Merit Protection Commissioner or a person authorised for the purposes of this section by the Merit Protection Commissioner.
- (c) an Agency Head or a person authorised for the purposes of this section by an Agency Head.<sup>104</sup>

13.90 The relationship between the above provision and s 70 of the *Crimes Act 1914* (Cth) is explained in the *APS Values and Code of Conduct in Practice*:

a public interest disclosure that is made in accordance with the [Public Service] Act and regulations (that is, to the relevant Agency Head, the Public Service Commissioner, the Merit Protection Commissioner or persons authorised by them) is not considered an unauthorised disclosure of information or an offence under s 70 of the *Crimes Act*.<sup>105</sup>

13.91 Accordingly, where an APS employee discloses information within the parameters of s 16 of the *Public Service Act*, he or she will not be liable to disciplinary action.

13.92 However, the scope of protection is not comprehensive. In particular, a disclosure will only fall within the scope of the provision where it raises a breach, or alleged breach, of the Code of Conduct. This excludes several types of disclosures that the House of Representatives Standing Committee on Legal and Constitutional Affairs, in its February 2009 report into whistleblowing protection within the Australian Government public sector, recommended should fall within the scope of public interest disclosure legislation—for example, a disclosure that alleges dangers to public health or safety, damage to the environment or wastage of public funds.<sup>106</sup> Section 16 only protects disclosures that an APS employee makes to the agency head, the Public Service Commissioner, the Merit Protection Commissioner or an authorised representative of one of these. The House of Representatives Standing Committee noted the need for a public interest disclosure system to provide multiple avenues for

---

104 *Public Service Act 1999* (Cth) s 16. Regulation 2.4(1) of the *Public Service Regulations* requires agency heads to establish procedures to manage whistleblowing reports in accordance with minimum requirements.

105 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <[www.apsc.gov.au](http://www.apsc.gov.au)> at 23 September 2008, 103.

106 The House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that the types of disclosures to be protected by the Public Interest Disclosure Bill should include serious matters related to: illegal activity; corruption; maladministration; breach of public trust; scientific misconduct; wastage of public funds; dangers to public health; dangers to public safety; dangers to the environment; official misconduct; and adverse action against a person who makes a public interest disclosure under the legislation. Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 7.

reporting disclosures and recommended that bodies authorised to receive and investigate public interest disclosures should also include the Commonwealth Ombudsman and integrity agencies.<sup>107</sup>

13.93 In its submission on IP 34, the CPSU stated that there was a ‘clear consensus’ among its members about the inadequacy of whistleblower protections in s 16 of the *Public Service Act*. The CPSU recommended that secrecy provisions in the *Public Service Act* should include an express exception dealing with protected disclosures.<sup>108</sup>

### **ALRC’s views**

13.94 The secrecy provisions in the *Public Service Act* should include a clear statement that individuals who make public interest disclosures in accordance with Commonwealth public interest disclosure legislation should be immune from administrative disciplinary penalties.

13.95 In this Discussion Paper, the ALRC has assumed that Commonwealth public interest disclosure legislation will be enacted and that the terms of this legislation will largely reflect the recommendations in the 2009 House of Representatives Standing Committee’s report. This legislation would provide immunity from liability under reg 2.1 for disclosures made in the public interest.

13.96 In Chapter 9, the ALRC proposes that the general secrecy offence should include a note cross-referencing to the immunity provided by Commonwealth public interest disclosure legislation.<sup>109</sup> However, if such legislation provides insufficient protection, or is not enacted, then the ALRC envisages that there may be a need to include an express public interest exception. The ALRC’s view is that the same approach should apply in the administrative context.

13.97 The ALRC has not been made aware of any issues with the exceptions currently set out in reg 2.1. These exceptions all appear to provide important limitations to the potential for an APS employee to be made subject to disciplinary action for the disclosure of Commonwealth information. The ALRC’s view, therefore, is that these exceptions should be retained. The exceptions are consistent with those included by the ALRC in the proposed general secrecy offence.<sup>110</sup>

**Proposal 13–4** Regulation 2.1 of the *Public Service Regulations 1999* (Cth) should include a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.

<sup>107</sup> Ibid, Ch 7, Recs 17, 18.

<sup>108</sup> Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

<sup>109</sup> Proposal 9–2.

<sup>110</sup> Proposal 9–1.

## Penalties

### Background

13.98 Under the *Public Service Act*, an agency head may impose one of the following penalties for a breach of the Code of Conduct: termination of employment; reduction in classification; re-assignment of duties; reduction in salary; deductions from salary, by way of fine, which is not to exceed 2% of the APS employee's annual salary;<sup>111</sup> and a reprimand.<sup>112</sup> Provided it is clearly cast as management action and not a penalty, an agency head also may prescribe other action in order to reduce the risk of further misconduct.<sup>113</sup>

13.99 Within these parameters, the decision whether to impose an administrative penalty for a breach of the Code of Conduct, and what type of administrative penalty to impose, are discretionary matters for each agency head. The House of Representatives Standing Committee on Legal and Constitutional Affairs noted that:

The culture of each organisation is a significant variable in any discussion concerning consistency in the application of administrative sanctions. Increased emphasis may be placed on the security of third party information in some departments than others because of the nature of a department's operation. For example, as officers of some departments are subject to legislation which imposes criminal sanctions on the disclosure of particular information, it may be expected that stronger disciplinary action would be taken against those officers than officers in other departments where penal sanctions do not exist.<sup>114</sup>

13.100 In its guide on handling misconduct, the APSC notes that the purpose of the Code of Conduct 'is to ensure effective administration and to maintain public confidence in the integrity of an organisation's processes and practices rather than to punish individuals'.<sup>115</sup> Sanctions for breach therefore 'should focus on reducing or eliminating the likelihood of future similar behaviour'.<sup>116</sup> The APSC goes on to advise that:

111 *Public Service Act 1999* (Cth) s 15; *Public Service Regulations 1999* (Cth) reg 2.3. Australian Parliament—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), 85 opposed an increase in the maximum fine payable under the *Public Service Act* on the basis that 'it would make the fine more akin to a criminal penalty than an administrative sanction'.

112 *Public Service Act 1999* (Cth) s 15.

113 Australian Public Service Commission, *Handling Misconduct: A Human Resources Practitioner's Guide to the Reporting and Handling of Suspected and Determined Breaches of the APS Code of Conduct* (2008), 55. In the context of unauthorised disclosure of information, this hypothetically could involve restricting an employee's access to certain information.

114 Australian Parliament—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), 81.

115 Australian Public Service Commission, *Handling Misconduct: A Human Resources Practitioner's Guide to the Reporting and Handling of Suspected and Determined Breaches of the APS Code of Conduct* (2008), 55.

116 Ibid.

Sanctions are intended to be proportionate to the nature of the breach, provide a clear message to the relevant employee that their behaviour was not acceptable, and act as a deterrent to the employee and others ... The sanction should focus on the seriousness of what the employee has done—the number of elements breached is not, of itself, a relevant consideration. Prior misconduct is also relevant to the imposition of a sanction and might usefully be taken into account by the sanction delegate where:

- it indicates that the employee was, or should have been, well aware of the standard of conduct expected and the potential consequences of misconduct
- it demonstrates that the employee is apparently unwilling to adhere to the standard of conduct expected.<sup>117</sup>

13.101 Termination of employment, for example, is considered by the APSC to be appropriate only where the misconduct is sufficiently serious that the employee should no longer remain in the APS; or where the employee has, by his or her actions, repudiated a basic element of the employment relationship.<sup>118</sup> The APSC advises that agencies should develop guidance materials, including an explanation of the penalties that can be imposed for breach of the Code of Conduct, factors to be considered in determining an appropriate penalty and agency-specific examples of the circumstances in which particular penalties may be appropriate.<sup>119</sup>

### **Submissions and consultations**

13.102 In IP 34, the ALRC asked whether the range and level of administrative penalties available for breaches of secrecy provisions committed by Commonwealth officers were adequate and appropriate.<sup>120</sup> The ALRC also questioned whether administrative penalties for breach of similar types of secrecy provisions were being applied consistently across Australian Government agencies.<sup>121</sup>

13.103 Only a small number of stakeholders made submissions on these questions. The AGD noted that the range and level of administrative penalties available for breaches of secrecy provisions by Commonwealth officers were the same as those that apply for all breaches of the Code of Conduct. Consistency of application is assisted by the APSC's guidance to agencies on the interpretation and application of the *Public Service Act*.<sup>122</sup> The AIC supported the range and level of administrative penalties currently available for breaches of secrecy provisions.<sup>123</sup>

---

117 Ibid, 56.

118 Ibid, 58. The APSC also discusses circumstances that could warrant a reduction in classification; reassignment of duties; reduction in salary; deductions from salary; and reprimand: 58–61.

119 Ibid, 62.

120 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–12.

121 Ibid, Question 5–15.

122 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

123 Australian Intelligence Community, *Submission SR 37*, 6 March 2009. ASIC advised that it has not had any instances of unauthorised disclosures that have given rise to the application of administrative penalties: Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

13.104 Liberty Victoria and Whistleblowers Australia were of the view that any penalties imposed for the unauthorised handling of information should be commensurate with the potential harm that could result from the disclosure.<sup>124</sup> The DHS commented that the range of penalties for breach of the Code of Conduct

should reflect the circumstances of the breach, the seniority of the employee, the seriousness of the consequences of the breach and whether the employee has breached the provision previously.<sup>125</sup>

### ALRC's views

13.105 The penalties that an Australian Government agency may impose on an APS employee who has breached a secrecy requirement in the *Public Service Act* are the same as those that apply to all other breaches of the APS Code of Conduct. Submissions to this Inquiry have not expressed particular concern about the range of penalties available. At this stage, the ALRC does not propose reform of the range of administrative penalties for breach of secrecy provisions.<sup>126</sup>

13.106 However, there is scope for clarifying the manner in which an agency will apply administrative penalties for breaches of secrecy provisions. In Chapter 15, the ALRC proposes that Australian Government agencies should develop and implement policies clarifying the application of relevant secrecy laws to their information holdings.<sup>127</sup> These policies may be useful in advising APS employees about the administrative penalties that could result from breach of a secrecy obligation, including the factors that will be considered in determining penalties, such as the potential harm caused to the agency by the circumstances of disclosure or the nature of the information, any prior unauthorised disclosures, and the seniority of the employee.

**Proposal 13–5** The information-handling policies developed by Australian Government agencies in accordance with Proposal 15–1 should clearly set out the disciplinary penalties that could result from breach of secrecy obligations, including the factors that will be considered in determining any such penalty.

<sup>124</sup> Whistleblowers Australia, *Submission SR 40*, 10 March 2009; Liberty Victoria, *Submission SR 19*, 18 February 2009.

<sup>125</sup> Department of Human Services, *Submission SR 26*, 20 February 2009.

<sup>126</sup> If changes are to be made to the administrative penalty framework, these should be considered as a part of an overall review of the Code of Conduct and related provisions. For example, the ALRC questions whether the cap on fines at 2% of the APS employee's annual salary is too low for this to be an effective penalty.

<sup>127</sup> Proposal 15–1.

## **Processes for dealing with breaches**

### **Background**

13.107 This final section of the chapter discusses various processes that an Australian Government agency must follow in making a determination that an APS employee has breached the requirements of the Code of Conduct, and the manner in which the agency can deal with a finding of breach. It also considers situations where an APS employee suspected of breaching a secrecy law may be subject to both administrative and criminal proceedings.

#### ***Determining breaches of the Code of Conduct***

13.108 The *Public Service Act* requires agency heads to establish procedures for determining whether an APS employee has breached the Code of Conduct. The Act sets out minimal requirements for such procedures—namely that they:

- (a) must comply with basic procedural requirements set out in Commissioner's Directions; and
- (b) must have due regard to procedural fairness; and
- (c) may be different for different categories of APS employees.<sup>128</sup>

13.109 Chapter 5 of the *Public Service Commissioner's Directions 1999* (Cth) requires:

- an APS employee to be given information, and a reasonable opportunity to make a statement, before a determination is made in relation to a suspected breach of the Code of Conduct;<sup>129</sup>
- the process for determining whether an APS employee has breached the Code of Conduct to be carried out informally and expeditiously;<sup>130</sup>
- an agency head to take reasonable steps to ensure that a person who determines whether an APS employee has breached the Code of Conduct is, and appears to be, independent and unbiased;<sup>131</sup> and
- a written record to be prepared noting the outcome of the investigation.<sup>132</sup>

13.110 The AGS has advised that the procedures set out in the *Public Service Act* and associated instruments are not an exhaustive statement of procedural fairness.

---

128 *Public Service Act 1999* (Cth) s 15(3). Agency heads also must take reasonable steps to ensure that employees have ready access to the documents that set out these procedures.

129 *Public Service Commissioner's Directions 1999* (Cth) cl 5.2.

130 Ibid cl 5.3.

131 Ibid cl 5.4.

132 Ibid cl 5.5.

Rather, the steps that will satisfy procedural fairness obligations will depend on the circumstances of each case.<sup>133</sup>

### **Suspension of employment and reassignment of duties**

13.111 An APS employee may be suspended from duties where the agency head believes on reasonable grounds that the employee has, or may have, breached the Code of Conduct and suspension is in the public, or the agency's, interest.<sup>134</sup>

13.112 Suspension is subject to the following conditions:

- other than in exceptional circumstances, suspension without remuneration is to be for no longer than 30 days;<sup>135</sup>
- the agency head must review the suspension at reasonable intervals;<sup>136</sup>
- the agency head must immediately end the suspension if he or she no longer believes on reasonable grounds that the APS employee has, or may have, breached the Code of Conduct, or that suspension is in the public, or agency's, interest;<sup>137</sup> and
- the agency head must immediately end the suspension if a sanction has been imposed on the employee for the relevant breach of the Code of Conduct.<sup>138</sup>

13.113 An agency head is normally required to exercise his or her powers of suspension having 'due regard for procedural fairness'.<sup>139</sup> This requirement need not apply where the agency head is satisfied, on reasonable grounds, that it would not be appropriate in the circumstances.<sup>140</sup> However, it would be unusual for a decision maker to be satisfied on a reasonable basis that according procedural fairness would be inappropriate. The AGS notes that:

It might be appropriate not to accord procedural fairness in circumstances where there is urgency or some overriding public interest, for example, safety concerns. Even in such cases, an opportunity to comment might properly be provided after the initial suspension, and any comments taken into account on a review of the suspension.<sup>141</sup>

---

133 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

134 *Public Service Regulations 1999* (Cth) reg 3.10.

135 Ibid reg 3.10(3).

136 Ibid reg 3.10(4).

137 Ibid reg 3.10(5).

138 Ibid reg 3.10(6).

139 Ibid reg 3.10(7).

140 Ibid.

141 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

13.114 An agency head also determines whether a suspension is to be with or without remuneration. Factors that may influence this decision include, for example, the seriousness of the suspected misconduct and the estimated duration of the misconduct proceedings.<sup>142</sup>

13.115 As an alternative to suspension, an agency head may temporarily reassign an employee's duties while the employee is investigated for a suspected breach of the Code of Conduct.<sup>143</sup>

#### ***Review of findings of breach***

13.116 An APS employee is entitled to seek review of an agency-level decision in most cases, other than where the employee's employment has been terminated, by applying to the Merit Protection Commissioner (MPC).<sup>144</sup> Where a person's employment has been terminated, the employee may seek redress under the *Workplace Relations Act 1996* (Cth). Employees also have the right to seek judicial review by the Federal Court of the agency-level decision.

13.117 The APS has noted that, in general terms, a review by the MPC will address:

- whether the agency's Code procedures comply with the Directions
- whether these procedures were substantially complied with by the agency in the course of determining whether there was a breach of the Code
- on the evidence available, what act or acts were committed by the relevant employee
- did they amount to a breach of the Code
- if yes, was the sanction appropriate in all the circumstances?<sup>145</sup>

13.118 The MPC is not empowered to make a binding decision as a result of a review of an employment action. Rather, the agency head must 'consider' the MPC's recommendation and make a decision whether to confirm, vary or set aside and substitute a new action for the action that was under review.<sup>146</sup> If the MPC is not satisfied with the response by the agency head, the MPC may report the matter to the

---

142 Australian Public Service Commission, *Handling Misconduct: A Human Resources Practitioner's Guide to the Reporting and Handling of Suspected and Determined Breaches of the APS Code of Conduct* (2008), 35. Other relevant considerations include: obligations under the *Financial Management and Accountability Act 1997* (Cth) and whether suspension without remuneration would give the employee an added incentive to cooperate with the investigation.

143 *Public Service Act 1999* (Cth) s 25.

144 *Public Service Regulations 1999* (Cth) reg 5.24. Some exceptions apply to reviewable actions, including where the affected person has applied to have the action reviewed by a court or tribunal, or for actions mentioned in sch 1 of the *Public Service Regulations*: reg 5.23(2).

145 Australian Public Service Commission, *Handling Misconduct: A Human Resources Practitioner's Guide to the Reporting and Handling of Suspected and Determined Breaches of the APS Code of Conduct* (2008), 74.

146 *Public Service Regulations 1999* (Cth) reg 5.32.

relevant Minister, the Prime Minister or Parliament.<sup>147</sup> In 2007–08, the MPC reported that ‘virtually all recommendations made in relation to applications for review of action were accepted in full by the relevant agency heads’.<sup>148</sup>

### **Concurrent administrative and criminal proceedings**

13.119 An APS employee suspected of breaching a secrecy law may be subject to both administrative and criminal proceedings.<sup>149</sup> In its Legal Briefing, *Misconduct in the Australian Public Service*, the AGS noted that:

Where an APS employee engages in conduct which can be both a breach of the Code and a breach of the criminal law, the agency needs to make a management decision about the handling of the case. This includes a decision as to whether the matter should be referred to the Australian Federal Police (the AFP) and/or the Director of Public Prosecutions (DPP) for criminal investigation and/or possible prosecution. If a criminal investigation or prosecution takes place, the agency needs to consider whether it should proceed with misconduct action or should defer any such action pending the outcome of the criminal investigation or prosecution.<sup>150</sup>

13.120 The APSC has advised that an agency generally should not proceed with a disciplinary action if the police or prosecuting authorities consider that this action could prejudice criminal proceedings.<sup>151</sup> Ultimately, however, the decision whether to proceed with administrative action in parallel with the criminal process is at the discretion of the relevant agency.

13.121 Concurrent criminal and disciplinary proceedings may give rise to practical difficulties—for example, in the context of an accused’s right to silence. An APS employee subject to Code of Conduct proceedings may decline to provide information on the basis of the privilege against self-incrimination.<sup>152</sup> However, as explained in a briefing note by the AGS:

Where the conduct in question involves a possible criminal offence, as well as breaches of the Code, there is no automatic rule that administrative action must await the outcome of the criminal proceedings. The fact that the employee chooses not to provide evidence or submissions in a misconduct process because of a concern to protect rights in relation to a current or possible future criminal process (such as the

147 *Public Service Act 1999* (Cth) s 33(6).

148 Australian Public Service Commissioner, *Annual Report 2007–08* (2008), 101.

149 The potential for a person to be subject to multiple proceedings for the same conduct is not unique to secrecy laws. The ALRC made a number of recommendations about multiple proceedings and multiple penalties in its report, Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Ch 11.

150 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

151 Advice from the AGS referred to in Australian Public Service Commission, *Handling Misconduct: A Human Resources Practitioner’s Guide to the Reporting and Handling of Suspected and Determined Breaches of the APS Code of Conduct* (2008), 16–17.

152 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor. However, in *Goreng Goreng v Jennaway*, Flick J noted uncertainty regarding the manner in which the right to silence operates upon an administrative decision-making process: *Goreng Goreng v Jennaway* (2007) 164 FCR 567, 571.

right to silence or the privilege against self-incrimination) does not prevent a misconduct process from proceeding.<sup>153</sup>

13.122 In *Goreng Goreng v Jennaway*,<sup>154</sup> the Federal Court considered whether an agency should postpone its review of an employee's suspension in connection with a Code of Conduct investigation. The applicant argued that, as she was choosing to exercise her right of silence in the associated criminal proceedings, she would be unable to participate fully in the administrative hearing. Flick J accepted that there was a 'very real risk that the applicant cannot address in detail the facts essential to both the review process and the criminal proceedings', and that the 'substantial overlap of facts and issues of credit' in the criminal and administrative proceedings resulted in 'real prejudice or injustice'.<sup>155</sup> However, this did not 'ordain the postponement, perhaps for an indefinite period, of an administrative process'.<sup>156</sup> In the absence of any legislative provisions to the contrary, Flick J held that whether or not administrative processes were postponed pending the resolution of criminal proceedings was a discretionary matter for the agency.

13.123 In its 2002 report, *Principled Regulation* (ALRC 95), the ALRC considered the necessary procedural safeguards to deal with concurrent criminal and civil penalty proceedings.<sup>157</sup> The ALRC commented that, although the double jeopardy principle has primarily been applied in the context of criminal punishment, the underlying rationale that a person should not be punished twice for substantially the same act

appears no less applicable to parallel civil penalty and criminal penalty ... for the same conduct. It seems to follow that, if one of the rationales and aims of double jeopardy is to protect against double punishment, and if civil penalties are, at least to some extent, punitive in nature, double jeopardy protection should be extended to subsequent civil penalty proceedings for the same conduct.<sup>158</sup>

13.124 The ALRC recommended that where legislation provides for exposure to parallel criminal proceedings and civil penalty proceedings for the same or substantially the same conduct, the legislation should also provide that:

- civil penalty proceedings against a person must be stayed if criminal proceedings for the same, or substantially the same, conduct are commenced, or have already been commenced, against that person;
- no, or no further, civil penalty proceedings may be taken against a person if that person has been convicted of that criminal offence; and

<sup>153</sup> P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

<sup>154</sup> *Goreng Goreng v Jennaway* (2007) 164 FCR 567.

<sup>155</sup> Ibid, [48].

<sup>156</sup> Ibid, [48]–[50].

<sup>157</sup> Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Ch 11.

<sup>158</sup> Ibid, [11.37].

- if the person is not convicted of that criminal offence, the civil penalty proceedings may be resumed.<sup>159</sup>

13.125 The ALRC also recommended that evidence of information given or documents produced by a person in civil penalty proceedings should not be admissible in criminal proceedings against the person for the same or substantially the same conduct.<sup>160</sup> This responded to concerns that:

where the same conduct attracts both civil penalty liability and criminal liability, the use of evidence in more than one proceeding blurs the important distinctions between the criminal and civil process. Importantly, the criminal standard of proof requires the prosecution to establish its case ‘beyond reasonable doubt’ whereas civil penalty proceedings are characterised by a variable standard of proof at or above the balance of probabilities.

Further, evidence collected in a civil penalty proceeding may be subject to less protection than the criminal process. The civil process utilises discovery and interrogatories in order to disclose relevant information and seek admissions of factual material. Criminal procedure, on the other hand, applies procedural protections to investigation and prosecution, and protections such as the privilege against self-incrimination. The accused is not required to specify its defence, discover documents or answer interrogatories before trial. To allow evidence given in civil penalty proceedings to be used without control in subsequent criminal proceedings would be unjust.<sup>161</sup>

13.126 In 2008, the NSW Industrial Relations Commission used similar reasoning to justify delaying unfair dismissal proceedings to await the outcome of related criminal proceedings:

Ordinarily, where the incident or incidents from which an employee was dismissed also involve criminal proceedings against him, any [unfair dismissal] application would be delayed to await the outcome of those criminal proceedings. There are a number of reasons why such a delay ... is appropriate. For one thing, the standard of proof before the Commission is the civil standard of the balance of probability and not the criminal standard of proof beyond reasonable doubt. ... Furthermore, there would be considerable logistical difficulties for [an] ... applicant in properly advancing a case, with the criminal proceedings hanging over his head. He would have a right of silence ... but the question remains whether, in the light of his right to remain silent, he would be in a position to present proper argument in his own behalf.<sup>162</sup>

<sup>159</sup> Ibid, Rec 11–2.

<sup>160</sup> Ibid, Rec 11–3.

<sup>161</sup> Ibid, [11.74]–[11.75].

<sup>162</sup> *Zonneveld v South Eastern Sydney and Illawarra Area Health Service* [2008] NSW IR Comm 1119.

## **Submissions and consultations**

### ***Processes for dealing with breaches***

13.127 In IP 34, the ALRC asked about the effectiveness of the processes set out in the *Public Service Act* and related instruments for dealing with suspected breaches of secrecy provisions.<sup>163</sup>

13.128 The AGD supported the processes set out in the *Public Service Act*, and advised that these provide a useful mechanism to deal with minor breaches or conduct that could, if left unchecked, lead to a more serious breach of a secrecy provision.<sup>164</sup> The Australian Securities and Investments Commission (ASIC) advised that it has not had any cases in which it has had recourse to the processes set out in the *Public Service Act* and related instruments for investigating and enforcing suspected breaches of secrecy provisions.<sup>165</sup>

13.129 The Australian Press Council noted that where a Commonwealth officer makes a public interest disclosure to the media, this frequently results in the imposition of severe administrative penalties, such as termination of employment. It submitted that, before a severe administrative penalty is imposed, the officer should have the opportunity to have his or her case heard by a court or tribunal that can adjudicate on questions of public interest and intent, as well as make findings of fact.<sup>166</sup>

### ***Concurrent administrative and criminal proceedings***

13.130 In IP 34, the ALRC asked whether there was a need for any safeguards to apply where secrecy provisions could give rise to both administrative and criminal proceedings. In particular, the ALRC questioned whether legislation should provide for a stay of administrative proceedings to accommodate current or future criminal actions.<sup>167</sup>

13.131 The Australian Press Council and PIAC supported a requirement for a stay of administrative proceedings pending the outcome of a concurrent criminal action.<sup>168</sup> However, other stakeholders expressed significant opposition. The AFP considered it to be unnecessary for an administrative process relating to the improper disclosure of information to be stayed pending the result of a criminal prosecution. To do so could constitute a ‘significant and unreasonable delay to the administrative process’.<sup>169</sup>

---

163 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–5.

164 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

165 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

166 Australian Press Council, *Submission SR 16*, 18 February 2009.

167 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–9.

168 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; Australian Press Council, *Submission SR 16*, 18 February 2009.

169 Australian Federal Police, *Submission SR 33*, 3 March 2009. The AFP further noted that its professional standards framework affords different evidence gathering powers, including coercive powers, and a lower burden of proof. Therefore, the outcome of an administrative process may be different to that in a parallel criminal proceeding.

13.132 The AGD was of the view that each agency should retain discretion to decide how to proceed on a case-by-case basis. The AGD noted that legal proceedings can be lengthy and requiring such a stay could impose an unnecessary burden on the person involved and the agency if they have to await the outcome of such proceedings before taking any administrative action.<sup>170</sup> ASIC suggested that a stay of administrative proceedings could create an ‘unreasonable and unnecessary’ exposure to further unauthorised disclosures.<sup>171</sup>

13.133 Liberty Victoria submitted that the right to silence represents

a fundamental part of our criminal justice system but one which is increasingly dispensed with in administrative proceedings. Where self incriminating information might be critical to Australia’s security, it is important that an administrative proceeding is not stayed pending the outcome of a criminal proceeding (where the privilege against self incrimination may prevent critical information from coming to light). However, where there is no bar to an admission in an administrative proceeding being used against an accused in a criminal proceeding, an accused may refuse to provide information critical to Australia’s security. It is therefore in Australia’s interests to ensure self incriminating information obtained in an administrative proceeding is not used against the same accused in a criminal proceeding.<sup>172</sup>

13.134 Other stakeholders also considered the potential use of information obtained through administrative proceedings. In the event that a stay were refused, PIAC suggested that consideration be given to providing for use and derivative use immunity to apply to any evidence given in such circumstances.<sup>173</sup> Whistleblowers Australia advised of the need for ‘a clear delineation between investigations carried out for a disciplinary process, as opposed to investigations in relation to criminal offences’.<sup>174</sup>

## ALRC’s views

### *Processes for dealing with breaches*

13.135 The ALRC has not been made aware of any particular concerns about the procedural requirements set out in the *Public Service Act* and related instruments for handling suspected breaches of secrecy provisions. Accordingly, the ALRC is not proposing reforms to these requirements.

170 Attorney-General’s Department, *Submission SR 36*, 6 March 2009. The Department noted with favour the current APSC guidelines, which recognise that an agency should not undertake administrative proceedings where a law enforcement agency considers this could be prejudicial to criminal proceedings.

171 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

172 Liberty Victoria, *Submission SR 19*, 18 February 2009.

173 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009. ASIC also suggested that restrictions may be imposed on the admissibility in criminal proceedings of any information provided by an accused during an administrative hearing: Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

174 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

### ***Concurrent administrative and criminal proceedings***

13.136 There are compelling arguments against requiring a stay of administrative proceedings pending the outcome of a concurrent criminal action. As stakeholders have noted, criminal proceedings are often lengthy. Delaying administrative proceedings for this period of time is likely to result in practical difficulties for an agency seeking to take administrative action, both in relation to the agency's immediate options for preventing the APS employee from making further unauthorised disclosures and successfully making out a breach of the administrative provision in the future.

13.137 The policy considerations applicable to concurrent administrative and criminal proceedings can be distinguished from those that apply to concurrent civil and criminal proceedings. A key rationale for the recommendation in ALRC 95 for an automatic stay of civil proceedings on the commencement of substantially similar criminal proceedings was a concern that a person could be punished twice for substantially the same act. This argument is not as compelling in the administrative disciplinary context. Rather than being punitive in nature, proceedings for a suspected breach of the Code of Conduct are directed towards the 'efficient administration' of the public service and the maintenance of 'public confidence'.<sup>175</sup> This has similarities with the protective function of professional disciplinary proceedings, as explained in *Pillai v Messiter [No 2]*:

The public needs to be protected from delinquents and wrong-doers within professions. It also needs to be protected from seriously incompetent professional people who are ignorant of basic rules or indifferent as to rudimentary professional requirements.<sup>176</sup>

13.138 In the ALRC's view, a mandatory stay of administrative proceedings is not an appropriate safeguard for concurrent administrative and criminal proceedings for breach of a secrecy provision.<sup>177</sup> The ALRC considers that a more suitable focus is ensuring the substantive fairness of such proceedings. Preventing evidence of information given or documents produced by an APS employee for the purpose of administrative proceedings from being admitted in related criminal proceedings goes a long way to addressing these procedural concerns.

13.139 In particular, inclusion of such a non-admissibility provision in the *Public Service Act* would facilitate the full participation of an APS employee in administrative

<sup>175</sup> Australian Public Service Commission, *Handling Misconduct: A Human Resources Practitioner's Guide to the Reporting and Handling of Suspected and Determined Breaches of the APS Code of Conduct* (2008), 55.

<sup>176</sup> *Pillai v Messiter [No 2]* (1989) 16 NSWLR 197, 201.

<sup>177</sup> The permissibility of concurrent criminal proceedings has also been accepted in the context of professional disciplinary proceedings. See, eg, *Legal Profession Act 2004* (NSW), which provides that 'a complaint may be made and dealt with even though the Australian legal practitioner concerned is the subject of proposed or current criminal or civil proceedings relating to the subject matter of the complaint': *Legal Profession Act 2004* (NSW) s 600. An equivalent provision is set out in *Legal Profession Act 2006* (NT) s 559.

proceedings regardless of any decision to take advantage of his or her right to silence in related criminal proceedings. It also recognises the distinctions between the evidentiary and procedural safeguards available in criminal and administrative proceedings, and thereby upholds the integrity of the criminal process.

13.140 The ALRC's proposal is framed consistently with provisions governing the non-admissibility of evidence obtained in civil proceedings in subsequent criminal proceedings.<sup>178</sup> These have been interpreted as providing a use, but not a derivative use, immunity. In ALRC 95, the ALRC supported this balance in the following terms:

It would seem fair that evidence obtained by discovery and proved to a civil standard in a civil proceeding cannot be used in a subsequent criminal proceeding in relation to the same conduct. It is also desirable that regulators, with their wide range of investigatory powers, should take care when gathering and using evidence. The operation of [the non-admissibility provision] means that when a regulator commences civil penalty proceedings it will have to be mindful of how it obtains and uses evidence so as not to preclude or undermine a later criminal proceeding.

On the other hand, it seems desirable that regulators should be able to adduce evidence flowing from a chain of inquiry started by evidence given in civil penalty proceedings. To prevent 'derivative use' would mean that in most cases commencing criminal proceedings would be frustrated. Therefore, if it became apparent during the course of civil proceedings that the conduct was worse than originally thought and criminal in nature, the criminal conduct could not be punished accordingly.<sup>179</sup>

13.141 In the ALRC's preliminary view, the same reasoning applies to concurrent administrative and criminal proceedings.

**Proposal 13–6** The *Public Service Act 1999* (Cth) should provide that evidence of information given or documents produced by an Australian Public Service employee for the purpose of administrative disciplinary proceedings with respect to secrecy obligations is not admissible in criminal proceedings against the employee for the same, or substantially the same, conduct.

<sup>178</sup> See, eg, *Water Act 2007* (Cth) s 154; *Corporations Act 2001* (Cth) s 1317Q.

<sup>179</sup> Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [11.81]–[11.82].



# **14. Regulating Beyond the *Public Service Act***

---

## **Contents**

Introduction	483
Commonwealth employees outside the APS	484
Members of the ADF	485
Members of the AFP	486
Employees of ASIO and ASIS	487
Employees and office holders of statutory authorities	488
Ministerial staff and employees of parliamentary departments	491
Submissions and consultations	494
ALRC's views	496
Former Commonwealth employees	499
Submissions and consultations	501
ALRC's views	502
Persons outside Commonwealth employment	503
Contracted service providers	504
Members of boards and committees	513
State and territory public sector employees	515
No relationship with the Commonwealth	518
Lawful and reasonable employer directions	519
ALRC's views	520

## **Introduction**

14.1 In Chapter 13, the ALRC discusses the administrative secrecy framework that applies to Australian Public Service (APS) employees engaged under the *Public Service Act 1999* (Cth). However, many individuals that have access to Commonwealth information are not APS employees. This includes individuals employed by or on behalf of the Commonwealth under another statutory regime; former employees of the Commonwealth; and individuals who are not, and have never been, in an employment relationship with the Commonwealth.

14.2 This chapter first considers the administrative secrecy framework that governs Commonwealth employees engaged under a statutory regime other than the *Public Service Act*. A particular focus of proposals is consolidating and harmonising these administrative secrecy obligations with the *Public Service Act* regime.

14.3 The chapter goes on to consider the secrecy obligations of former Commonwealth employees and other individuals who have never been in an employment relationship with the Commonwealth, and options for enforcing these obligations. The chapter makes a number of proposals to ensure that individuals who fall outside the various administrative regimes but have, or have had, access to Commonwealth information are constrained by contractual obligations, or are made aware of their obligations of confidentiality under the general law. In particular, the proposals are directed towards impressing on those who access Commonwealth information the personal nature of secrecy obligations.

14.4 The final section of this chapter discusses the administrative secrecy obligations of Commonwealth employees other than those expressly set out in their terms and conditions of employment—in particular, lawful and reasonable directions issued by Australian Government agencies.

## **Commonwealth employees outside the APS**

14.5 As discussed in detail in Chapter 13, the *Public Service Act* and related instruments establish a comprehensive administrative secrecy regime for APS employees.<sup>1</sup> Regulation 2.1 of the *Public Service Regulations 1999* (Cth) imports into the APS Code of Conduct a duty on APS employees not to disclose official information in certain circumstances—in particular, where disclosure could harm the effective working of government.<sup>2</sup> Exceptions to the application of the secrecy requirement include, for example, where the disclosure was in the course of the APS employee’s duties,<sup>3</sup> or the information was disclosed in accordance with an authorisation by the agency head.<sup>4</sup> The *Public Service Act* specifies the administrative disciplinary penalties that an agency head may impose when an APS employee is found to have breached the APS Code of Conduct. The Act also requires agency heads to comply with procedural safeguards when investigating and enforcing breaches.

14.6 However, many Commonwealth employees, including those who may handle the most sensitive Commonwealth information, fall outside the ambit of the *Public Service Act* and therefore are not subject to the APS Code of Conduct. These include:

- members of the Australian Defence Force (ADF);
- members of the Australian Federal Police (AFP);

1 An APS employee is defined in s 7 of the *Public Service Act 1999* (Cth) to mean a person engaged under s 22—that is, a person engaged by an Agency Head for the purposes of the agency—or under s 72—that is, a person engaged as an APS employee by the Public Service Commissioner in a specified agency as the result of an administrative rearrangement. An agency is defined in s 7 to mean a department, an executive agency established by the Governor-General, or a statutory agency.

2 Proposals 13–1 to 13–3 propose reforms to the secrecy requirements in reg 2.1 of the *Public Service Regulations 1999* (Cth).

3 Ibid reg 2.1(5)(a).

4 Ibid reg 2.1(5)(b).

- employees of the Australian Security Intelligence Organisation (ASIO) and the Australian Security Intelligence Service (ASIS);
- employees and office holders of statutory authorities and corporations; and
- ministerial staff and employees of parliamentary departments.

14.7 The disciplinary framework that applies to these employees is summarised below.

### **Members of the ADF**

14.8 The *Defence Force Discipline Act 1982* (Cth) (DFD Act) establishes the disciplinary regime applicable to ADF members. There are two secrecy provisions in the DFD Act. Section 16 prohibits communicating with, or giving intelligence to, the enemy. Section 58 prohibits the unlawful disclosure of information likely to be prejudicial to the defence or security of Australia.

14.9 Responsibility for investigating suspected breaches of the DFD Act rests with the service police forces under the overall command of the Provosts-Marshall. Service police forces decide whether or not to investigate incidents, refer offences to civilian criminal authorities for investigation, and, when required, conduct investigations and provide evidence to support prosecutions of service offences.<sup>5</sup>

14.10 The manner in which a charge for breach of the DFD Act is dealt with—and the potential punishment for any finding of breach—depends on the ‘service tribunal’ to which the hearing of the breach is allocated: a summary authority, or the Australian Military Court (AMC).<sup>6</sup> Summary authorities comprise officers of the ADF. They try service offences in a manner broadly akin to a civilian criminal trial, in accordance with detailed procedural requirements set out in the *Summary Authority Rules 2008* (Cth). Although the Rules reflect many of the due process requirements of the general law, there are also some significant departures. For example, while an accused person has a right to representation by a member of the ADF, there is no automatic right to a legal representative.

14.11 The AMC is a permanent military court independent of the ADF chain of command. The AMC is comprised of military judges, who are serving members of the ADF appointed by the Minister. Depending on its seriousness, an offence may be dealt with by a military judge alone, or by a military judge and military jury. Proceedings in the AMC are conducted in accordance with the *Australian Military Court Rules 2007* (Cth).

---

5 Parliament of Australia—Senate Foreign Affairs Defence and Trade References Committee, *The Effectiveness of Australia’s Military Justice System* (2005), [3.8].

6 The *Defence Force Discipline Act* also provides for the appointment of Discipline Officers to deal with minor infractions: *Defence Force Discipline Act 1982* (Cth) pt IXA.

14.12 The DFD Act sets out the punishments that a service tribunal may impose on a convicted person. These range in severity from imprisonment for life or for a specified period, to dismissal or suspension from the ADF, reduction in rank or reprimand.<sup>7</sup>

### **Members of the AFP**

14.13 The *Australian Federal Police Act 1979* (Cth) (AFP Act) and the *Australian Federal Police Categories of Conduct Determination 2006* (Cth) establish the disciplinary regime relevant to AFP appointees.<sup>8</sup>

14.14 The AFP Act sets out the overarching disciplinary framework for misconduct by AFP appointees. The Act provides for four categories of AFP conduct issues of escalating seriousness:<sup>9</sup>

- Category 1: inappropriate conduct that relates to minor management or custom service matters, or reveals a need for improvement in performance, and does not warrant being treated as category 2 or 3 conduct;<sup>10</sup>
- Category 2: minor misconduct or inappropriate conduct that reveals unsatisfactory behaviour which would otherwise be category 1 conduct but warrants, because of its repeated nature, to be treated as category 2 conduct;<sup>11</sup>
- Category 3: serious misconduct, conduct that raises the question whether termination action should be taken; or conduct that involves a breach of the criminal law or serious neglect of duty, apart from conduct that raises a corruption issue;<sup>12</sup> and
- Conduct giving rise to a corruption issue.

14.15 The conduct that falls within categories 1, 2 and 3 is described in the *Australian Federal Police Categories of Conduct Determination*. Breach of a secrecy provision could amount to category 2 conduct if it involves ‘accidental or unintentional access or disclosure of information which the AFP appointee had a duty not to disclose or should not have had access’.<sup>13</sup> A more serious breach could fall within category 3 conduct if it involves: ‘improperly disclosing or failing to protect from improper disclosure, sensitive information held by the AFP’, ‘unlawfully or improperly accessing AFP

7 Ibid s 68(1).

8 An AFP appointee is defined to include: a Deputy Commissioner; an AFP employee; a special member; or a special protective service officer: see *Australian Federal Police Act 1979* (Cth) s 4.

9 Ibid s 40RK. As discussed below, the content of these misconduct categories is described in the *Australian Federal Police Categories of Conduct Determination 2006* (Cth).

10 *Australian Federal Police Act 1979* (Cth) s 40RN.

11 Ibid s 40RO.

12 Ibid s 40RP.

13 *Australian Federal Police Categories of Conduct Determination 2006* (Cth), sch.

information', or breaching any criminal law other than one relating to Commonwealth fraud.<sup>14</sup>

14.16 Category 1 and 2 conduct issues are dealt with by an appointee's supervisor. The AFP Act sets out detailed procedural requirements for handling these issues.<sup>15</sup> These include requirements for a manager to ensure that the AFP officer and the complainant (if any) have an adequate opportunity to be heard in relation to the issue; and to ensure that the AFP officer is involved, as far as practicable, in the resolution of the issue. Where a manager is satisfied, on reasonable grounds, that an AFP appointee has engaged in Category 2 conduct, the manager may take remedial action, training and development action, or both, against the appointee.<sup>16</sup>

14.17 More formal investigation processes apply to category 3 conduct and corruption issues. Investigations are conducted by an allocated officer of an AFP unit specifically constituted to undertake investigations of misconduct by AFP appointees.<sup>17</sup> The Commonwealth Ombudsman must be notified of any investigation of a category 3 conduct issue.<sup>18</sup> Where an investigator is satisfied, on reasonable grounds, that an AFP appointee has engaged in Category 3 conduct, the investigator may recommend any one or more of the following: termination; remedial action; training and development action; or any other action that the Commissioner can take in relation to the AFP appointee.<sup>19</sup>

### **Employees of ASIO and ASIS**

14.18 Unlike other officers of the Australian Intelligence Community (AIC),<sup>20</sup> employees of ASIO and ASIS are not employed under the *Public Service Act*. The *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) provides the legislative basis for the employment of ASIO employees. The *Intelligence Services Act 2001* (Cth) provides the legislative basis for the employment of ASIS employees. While ASIO and ASIS employees are subject to criminal secrecy offences,<sup>21</sup> no express administrative secrecy obligations or penalties are set out in their respective legislation.

---

14 Ibid.

15 *Australian Federal Police Act 1979* (Cth) pt V div 3 subdiv C.

16 Ibid s 40TJ.

17 Ibid s 40RD. Where the issue relates to a member of the section, or it would otherwise be inappropriate for the issue to be investigated by a member of the unit, the Commissioner must allocate the issue to a suitably qualified person who is not a member of the unit: s 40TO.

18 Ibid s 40TM(1).

19 Ibid s 40TR.

20 The AIC covers the Office of National Assessments (ONA), ASIO, ASIS, the Defence Intelligence Organisation (DIO), the Defence Signals Directorate (DSD) and the Defence Imagery and Geospatial Organisation (DIGO).

21 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18; *Intelligence Services Act 2001* (Cth) s 39. ASIO and ASIS employees are also subject to the general secrecy offences in ss 70 and 79 of the *Crimes Act 1914* (Cth).

14.19 Under s 86 of the ASIO Act, the terms and conditions of employment of officers and employees of ASIO ‘are determined from time to time by the Director-General’. The Act provides only minimal requirements for such employment conditions—principally, that an officer’s employment can only be terminated in accordance with a term or condition of his or her employment.<sup>22</sup> While information on ASIO’s terms and conditions of employment is not publicly available, ASIO advises that ‘ASIO’s conditions of service are similar to those of the Australian Public Service’.<sup>23</sup>

14.20 The *Intelligence Services Act* is somewhat more prescriptive as regards the terms and conditions of ASIS employment. As with ASIO, the Director-General of ASIS may determine the terms and conditions on which employees are to be employed. However, the Director-General of ASIS is obliged to consult with affected employees about these conditions.<sup>24</sup> Further, the Act prescribes that:

Although employees of ASIS are not employed under the *Public Service Act 1999*, the Director-General must adopt the principles of that Act in relation to employees of ASIS to the extent to which the Director-General considers they are consistent with the effective performance of the functions of ASIS.<sup>25</sup>

14.21 The Director-General is also under an obligation to establish staff grievance procedures, adopting the principles of the *Public Service Act* to the extent that they are consistent with the effective performance of the functions of ASIS.<sup>26</sup> The procedures must include:

- (a) initial consideration of grievances by the Director-General or a person authorised in writing by the Director-General; [and]
- (b) establishment of Grievance Review Panels chaired by independent Chairs to make determinations reviewing initial consideration of grievances.<sup>27</sup>

### **Employees and office holders of statutory authorities**

14.22 A Commonwealth statutory authority can be defined as any public sector entity created by a specific law of the Commonwealth.<sup>28</sup> In accordance with this definition, there are over 160 statutory authorities in the Commonwealth sphere, with diverse legal frameworks and governance structures.<sup>29</sup> There is variation in whether the

22 *Australian Security Intelligence Organisation Act 1979* (Cth) s 89. Section 90 of the Act also provides that the regulations may deal with matters relating to employment conditions for temporary and casual staff. No such regulations have been made.

23 Australian Security and Intelligence Organisation, *Conditions of Service* (2008) <[www.asio.gov.au/Careers/Content/Conditions.aspx](http://www.asio.gov.au/Careers/Content/Conditions.aspx)> at 10 October 2008. The similarities between the terms and conditions of employment for ASIO staff and APS employees was also noted in the submission by the AIC on IP 34: Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

24 *Intelligence Services Act 2001* (Cth) s 33.

25 Ibid s 355.

26 Ibid s 37.

27 Ibid s 37(3). The Director-General also must implement a determination of a Grievance Review Panel to the extent that it is within his or her power to do so. *Intelligence Services Act 2001* (Cth) s 37(4).

28 J Uhrig, *Review of the Corporate Governance of Statutory Authorities and Office Holders* (2003).  
29 Ibid.

authority is an agency prescribed under the *Financial Management and Accountability Act 1997* (Cth) (FMA Act)<sup>30</sup> or an authority subject to the *Commonwealth Authorities and Companies Act 1997* (Cth) (CAC Act).<sup>31</sup> Every Commonwealth statutory authority must operate in accordance with the governance framework set out in one of these Acts.

14.23 The functions performed by statutory authorities also vary widely. For example, some of the statutory authorities subject to the CAC Act, such as the ALRC, undertake a public policy function, largely separate from the commercial sphere. Others, such as the Australian Postal Corporation, undertake functions that are more closely akin to business activities in the private sector. Professor Roger Wettenhall has commented on the lack of a clear classification system for public sector entities, and the challenges that this creates:

We all know that structures abound with formal titles such as ‘department’, ‘division’, ‘bureau’, ‘commission’, ‘council’, ‘authority’ and so on, but we lack a classificatory system which might align such apparent class-names with agreed sets of purposes or operating conditions. There is room for confusion when a department here seems to be discharging similar functions to a bureau or a commission there, or when a board is renamed a commission simply as a sort of rejuvenating exercise, without major structural redesign. Equally unhelpfully, moderns in the [New Public Management] tradition sometimes abandon explanatory class-names altogether—as in recent Australian cases such as Transport Australia, Environment Australia, or Planning and Land Management.<sup>32</sup>

14.24 The conduct requirements—including the secrecy obligations—that apply to employees of Commonwealth statutory authorities depend on the status of the employing authority under the *Public Service Act*. For many statutory authorities, the statutory office holder and his or her staff constitute a ‘statutory agency’ within the meaning of the *Public Service Act*.<sup>33</sup> In such cases, the administrative framework in the *Public Service Act* applies—including the APS Code of Conduct and procedures for suspected breaches of the Code.

14.25 For statutory authorities that employ staff other than under the *Public Service Act*, the terms and conditions of employment are usually left to a Certified Agreement

30 Schedule 1 of the *Financial Management and Accountability Regulations 1997* (Cth) lists 85 bodies that are ‘prescribed agencies’ for the purpose of the *Financial Management and Accountability Act 1997* (Cth).

31 The CAC Act defines ‘Commonwealth authority’ as a body created by legislation with a separate legal identity from the Commonwealth and with the power to hold money on its own account: *Commonwealth Authorities and Companies Act 1997* (Cth) s 7.

32 R Wettenhall, ‘Exploring Types of Public Sector Organizations: Past Exercises and Current Issues’ (2003) 3 *Public Organization Review* 219, 1–2.

33 The Australian Public Service Commission (APSC) has issued a list of all Australian Public Service Agencies, including statutory agencies that employ some or all of their staff under the *Public Service Act 1999* (Cth): Australian Public Service Commission, *Australian Public Service Agencies* (2009) <[www.apsc.gov.au/apsprofile/agencies.htm](http://www.apsc.gov.au/apsprofile/agencies.htm)> at 31 March 2009. As at 12 February 2009, there were 63 statutory agencies that employed all staff under the *Public Service Act*. A further 14 statutory agencies had dual staffing powers.

or the discretion of the authority itself (or a particular person or persons within the authority).<sup>34</sup> The terms and conditions of appointment of statutory office holders generally are at the discretion of the responsible minister or the Governor-General.<sup>35</sup>

14.26 The terms and conditions of employment for some, but not all, statutory authorities include express secrecy obligations. These differ in respect of their level of detail and the degree to which they diverge from the APS Code of Conduct. Differences also arise with regard to the administrative penalties made available to the authority and the processes for dealing with suspected breaches. For example, one of the Key Performance Indicators in the Employee Collective Agreement for the Australian Institute of Criminology is that ‘staff [will] conduct themselves in a manner which is consistent with the Public Service Code of Conduct’.<sup>36</sup>

14.27 Somewhat more targeted requirements are set out in the terms and conditions of employment for the Australian Prudential Regulation Authority (APRA). Section 48AC of the *Australian Prudential Regulation Authority Act 1998* (Cth) (APRA Act) requires that the Chair must determine a Code of Conduct for APRA, but does not include any guidance on the content of the Code.<sup>37</sup> The APRA Code of Conduct was issued on 1 July 2007 and includes a provision about information handling:

If you have access to confidential or sensitive information you should respect that confidentiality/sensitivity. You should take care to follow correct procedures, to ensure that information is not released to any unauthorised parties, including those who could seek to benefit financially or in other ways from its disclosure. Your attention is drawn to sections 56 and 57 of the *Australian Prudential Regulation Authority Act 1998* that relate to secrecy and to sections 70 and 79 of the *Crimes Act 1914*. Copies of the sections are available from the General Manager Human Resources.<sup>38</sup>

14.28 The APRA Code also includes a number of procedures that are ‘designed to ensure that a staff member under investigation is treated fairly and is given a reasonable opportunity to respond to allegations’. In particular, the Code provides that:

---

<sup>34</sup> The enabling legislation for some statutory authorities impose aspirational requirements for these terms and conditions of employment. For example, the *Australian Postal Corporation Act 1989* (Cth) requires Australia Post to ‘endeavour to achieve and maintain high standards as an employer in relation to terms and conditions of employment, occupational health, industrial safety, industrial democracy, non-discriminatory employment practices and other matters’: s 90. See also *Australian Broadcasting Corporation Act 1983* (Cth) ss 32, 33; *Special Broadcasting Service Act 1991* (Cth) ss 54, 55.

<sup>35</sup> In some situations, the terms and conditions of appointment are set by, or on the advice of, the Remuneration Tribunal: Remuneration Tribunal, *About the Remuneration Tribunal* (2009) <<http://www.remunerationtribunal.gov.au>> at 7 May 2009.

<sup>36</sup> Australian Institute of Criminology, *Employee Collective Agreement 2006–2009* (2006) <<http://www.aic.gov.au/institute/agreement/agreement.pdf>> at 7 April 2009, cl 37.

<sup>37</sup> *Australian Prudential Regulation Authority Act 1998* (Cth) s 48AC.

<sup>38</sup> Australian Prudential Regulation Authority, *APRA Code of Conduct* (2007) <<http://www.apra.gov.au/AboutAPRA>> at 4 March 2009 under ‘Standards of Conduct’.

Prior to any decision about action [for breach of the standards of conduct] being taken, there will be discussion with the staff member concerned who will be given the opportunity to respond to any allegations. Where a serious breach of conduct is involved the staff member may be required to attend a formal interview. Any person or organisation they choose may represent the staff member at this interview. In all cases, the decision reached is to be documented and the staff member informed of the outcome without undue delay.<sup>39</sup>

14.29 The APRA Code provides for a range of administrative penalties ranging from counselling or mediation for minor breaches through to transfer from a position, suspension from duty, exclusion from a performance payment or a reduction in pay or classification level for more serious or ongoing breaches. Provided a member of APRA's Executive Group gives approval, an employee may be dismissed for major breaches or a failure to heed reprimands or warnings.<sup>40</sup>

14.30 Part 3 div 4 of the CAC Act sets out some of 'the most significant duties' of officers and employees of Commonwealth authorities governed by that Act.<sup>41</sup> These provisions are a mix of civil and criminal penalty provisions. The ALRC has not classified any of these provisions as secrecy provisions. However, s 22 imposes an obligation on officers and employees to exercise their powers with care and diligence and in good faith; and ss 24 and 25 impose an obligation not to use their position—or information gained because of their position—to gain personal advantage or cause detriment to the Commonwealth or to another person.<sup>42</sup> These are civil penalty provisions. Where a court has determined that an officer has contravened one of these obligations, the relevant minister may apply for a pecuniary penalty order in an amount of up to \$200,000. In making such an order, the court must be satisfied that the contravention 'materially prejudices the interests of the Commonwealth authority or Commonwealth company'; 'materially prejudices the ability of the Commonwealth authority or Commonwealth company to pay its creditors'; or 'is serious'.<sup>43</sup>

14.31 No equivalent obligations or penalties are set out in the FMA Act.

## **Ministerial staff and employees of parliamentary departments**

### ***Employees of parliamentary departments***

14.32 The parliamentary departments—being the Department of the Senate, the Department of the House of Representatives and the Department of Parliamentary

---

39 Ibid, 19.

40 Any other disciplinary actions, with the exception of formal warnings, must be approved by the relevant Executive General Manager: Ibid, 18.

41 *Commonwealth Authorities and Companies Act 1997* (Cth) s 21.

42 The Act also sets out criminal offences for officers who are reckless or intentionally dishonest in exercising their powers, or use their position, or information gained from their position, with the intention of gaining an advantage for themselves or causing detriment to the Commonwealth or another, or recklessly as to whether they or another would gain an advantage or cause such detriment: s 26.

43 *Commonwealth Authorities and Companies Act 1997* (Cth) sch 2 cl 3.

Services—provide information, advice and support to the Houses of Parliament, and to committees, senators and members.

14.33 Prior to 1999, employees of the parliamentary departments were governed by the same legislation as the APS.<sup>44</sup> This changed with the introduction of the *Parliamentary Service Act 1999* (Cth), which

establishes a separate and independent framework for the employment of staff in the Parliamentary Departments. The framework follows that established by the *Public Service [Act]* except where differences are necessary to reflect the unique character of the parliamentary service and the obligation of parliamentary staff to serve the Parliament.<sup>45</sup>

14.34 Under the *Parliamentary Service Act*, employees of parliamentary departments must comply with the Parliamentary Service Code of Conduct.<sup>46</sup> Many of the obligations imposed by this Code are equivalent to those set out in the APS Code of Conduct.<sup>47</sup> For example, a parliamentary department employee is under a duty to comply with all applicable Australian laws when acting in the course of his or her employment;<sup>48</sup> and to maintain ‘appropriate confidentiality’ about dealings that he or she has with Houses of Parliament and parliamentary committees and their members.<sup>49</sup>

14.35 The Parliamentary Service Code of Conduct also requires employees to ‘comply with any other conduct requirement that is made by either House of the Parliament or by determinations’.<sup>50</sup> Clause 2.3.1 of *Parliamentary Service Determination 2003/2* (Cth) provides that:

Parliamentary Service employees must not, directly or indirectly, give or disclose to any person any information about the affairs of any other person or body which they acquire in the course of their employment unless:

- (i) they are required to do so in the course of their duties; or
- (ii) they have the Secretary’s express authority to do so.

14.36 Section 15 of the *Parliamentary Service Act* sets out an exhaustive list of the penalties that a secretary may impose on a parliamentary service employee who breaches the Code of Conduct.<sup>51</sup> Procedures for determining whether an employee has breached the Code of Conduct must ‘have due regard for procedural fairness’ and

---

44 The governing Act was the *Public Service Act 1922* (Cth).

45 Explanatory Memorandum, Parliamentary Service Bill 1999 (Cth), 1.

46 *Parliamentary Service Act 1999* (Cth) s 13.

47 *Public Service Act 1999* (Cth) s 13.

48 *Parliamentary Service Act 1999* (Cth) s 13(4).

49 Ibid s 13(6).

50 Ibid s 13(13).

51 Ibid s 15(1) provides that these are: termination of employment; reduction in classification; re-assignment of duties; reduction in salary; deductions from salary, by way of fine; and a reprimand.

comply with any requirements in a direction from the Parliamentary Service Commissioner.<sup>52</sup>

#### **Staff of ministers and other members of Parliament**

14.37 People employed by Members of Parliament (including ministers and other parliamentary office-holders) are engaged under the *Members of Parliament (Staff) Act 1984* (Cth) (MOPS Act). As at 1 June 2008, 1,374 people were employed under the MOPS Act.<sup>53</sup>

14.38 In its 2003 inquiry into the framework for employment and the management of staff under the MOPS Act,<sup>54</sup> the Senate Finance and Public Administration References Committee remarked on the ‘almost complete control’ the Act gives the Prime Minister over the conditions of employment for MOPS staff—including the power to determine whether a parliamentarian may employ staff; and to set and vary the terms and conditions of employment of staff.<sup>55</sup> The MOPS Act itself does not directly impose any secrecy obligations on employees, nor is the ALRC aware of such obligations arising as a consequence of other employment frameworks for MOPS staff, other than those arising under the general law.<sup>56</sup>

14.39 In the specific context of ministerial staff, however, additional conduct requirements apply. The *Code of Conduct for Ministerial Staff* was tabled in Parliament on 26 June 2008 and came into operation on 1 July 2008,<sup>57</sup> setting out the standards that ministerial staff are expected to meet in the performance of their duties. Many of these standards are essentially the same as those set out in the APS Code of Conduct and the Parliamentary Service Code of Conduct.<sup>58</sup> Other conduct requirements are specifically tailored to issues arising out of the particular functions of ministerial staffers, such as a requirement for staff to ‘acknowledge that ministerial

---

52 Ibid s 15(3).

53 Department of Finance and Deregulation, *Members of Parliament (Staff) Act 1984 Annual Report 2007–08*, 1.

54 This Inquiry had its genesis in the Inquiry of the Senate Select Committee on a Certain Maritime Incident (the ‘children overboard’ affair).

55 Parliament of Australia—Senate Finance and Public Administration References Committee, *Staff Employed under the Members of Parliament (Staff) Act 1984* (2003), [2.13]. The Prime Minister may also issue directions under the *Public Service Act 1999* (Cth) s 21. These have been used, for example, to preserve a right of return for APS employees who have taken a position as a MOPS employee: *Prime Minister’s Public Service Directions 1999* (Cth).

56 As at November 2008, three types of employment relationships were in place for employees under the MOPS Act: Individual Australian Workplace Agreements, for employees above the level of Adviser; Determination 2007/PM/1 under the MOPS Act, *Terms and Conditions of Employment for Employees Above the Level of Adviser*; and the *Commonwealth Members of Parliament Staff Collective Agreement 2006–09*, for employees at or below the level of Adviser: Department of Finance and Deregulation, *Members of Parliament (Staff) Act 1984 Annual Report 2007–08*, 3.

57 J Faulkner (Cabinet Secretary and Special Minister of State), *Code of Conduct for Ministerial Staff* (2008) <[http://www.smos.gov.au/media/code\\_of\\_conduct.html](http://www.smos.gov.au/media/code_of_conduct.html)> at 31 March 2009.

58 Ibid, cl 1, 2, 3 provides, eg, that staff must: behave honestly and with integrity in the course of their employment; act with care and diligence in the performance of their duties; and disclose and take reasonable steps to avoid any conflict of interest in connection with their employment.

staff do not have the power to direct APS employees in their own right and that APS employees are not subject to their direction'.<sup>59</sup>

14.40 The *Code of Conduct for Ministerial Staff* does not include a secrecy provision equivalent to reg 2.1 of the *Public Service Regulations 1999* (Cth) (or the related duty in the Parliamentary Service Code of Conduct). The Code does, however, require ministerial staff to 'maintain appropriate confidentiality about their dealings with their Minister, other Ministers, other Ministerial staff, and APS and Parliamentary Service employees'.<sup>60</sup>

14.41 The Senate Finance and Public Administration Reference Committee has supported distinguishing between the conduct requirements of ministerial staff and other MOPS employees in the following terms:

Ministerial advisers are in many ways functionally the same as public servants: they are employees of the executive arm of government, there to implement the government's policies. This is why in most jurisdictions ... ministerial staff are public servants subject to a number of special conditions. It is their attachment to the executive arm that distinguishes them from all other MOPS employees, who, even though they may have partisan loyalties, serve the needs of their employer as a Member of Parliament.<sup>61</sup>

## **Submissions and consultations**

### ***Framing the administrative secrecy requirements***

14.42 The ALRC did not ask a specific question in the Issues Paper, *Review of Secrecy Laws* (IP 34),<sup>62</sup> about the administrative secrecy obligations that should apply to Commonwealth employees other than those employed under the *Public Service Act*. Several stakeholders, however, made comments that are relevant to this issue.

14.43 Ron Fraser suggested that administrative secrecy requirements should apply consistently across all Australian Government agencies.<sup>63</sup> James Renwick submitted that, because leaks often come from ministerial offices, secrecy laws should apply to ministerial staff in addition to Commonwealth public servants.<sup>64</sup>

14.44 The Australian Securities and Investments Commission (ASIC) advised that it employs staff under s 120(3) of its Act, in addition to staff employed under the *Public Service Act*. ASIC includes a clause in its contracts of employment that requires those

---

59 Ibid, cl 11.

60 Ibid, cl 15.

61 Parliament of Australia—Senate Finance and Public Administration References Committee, *Staff Employed under the Members of Parliament (Staff) Act 1984* (2003), [5.5].

62 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

63 R Fraser, *Submission SR 42*, 23 March 2009.

64 J Renwick, *Submission SR 02*, 11 December 2008.

engaged under s 120(3) to comply with the APS Code of Conduct and other ASIC policies and procedures. Failure to do so may lead to termination of the contract.<sup>65</sup>

14.45 The Community and Public Sector Union (CPSU) focused on the protection of those who make public interest disclosures, and expressed concern that this category could be artificially constrained to persons directly engaged by APS agencies. The CPSU submitted that all administrative secrecy requirements that apply to Commonwealth employees should include an exception for public interest disclosures.<sup>66</sup>

#### ***Processes for investigation and enforcement***

14.46 In IP 34, the ALRC asked how effective the processes were for dealing with breaches of secrecy laws by Commonwealth officers other than APS employees. In particular, the ALRC questioned whether the legislation under which these officers were employed should adopt the processes for dealing with misconduct set out in the *Public Service Act*. The ALRC also asked whether there should be a process for merits review of any penalties imposed.<sup>67</sup>

14.47 The Public Interest Advocacy Centre (PIAC) agreed that procedures modelled on those that apply to APS employees should be adopted generally for Commonwealth officers, and that an avenue for merits review should be made available.<sup>68</sup> The Australian Government Attorney-General's Department (AGD) submitted that it

can see value in such processes being generally consistent with similar processes that are applicable to APS employees. The majority of disciplinary processes for non-APS Commonwealth officers incorporate natural justice principles, such as the ability to respond to allegations and options for reconsideration of a decision. Where there is no merits review of penalties imposed on non-APS Commonwealth officers, consideration could be given to the appropriateness of introducing such a process.<sup>69</sup>

14.48 The Australian Intelligence Community advised that,

Where an agency's officers are not employed under the *Public Service Act 1999*, equivalent conditions of service are put in place under that agency's administrative arrangements. For example, in accordance with section 35 of the *Intelligence Services Act*, ASIS adopts the principles and ethics of the Australian Public Service to the extent the Director-General considers they are consistent with the effective performance of the functions of ASIS. Similar arrangements exist for ASIO employees, who are employed under the *ASIO Act*.<sup>70</sup>

65 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

66 Community and Public Sector Union, *Submission SR 32*, 2 March 2009. Public interest disclosures are discussed in Ch 9.

67 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–6.

68 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

69 Attorney-General's Department, *Submission SR 36*, 6 March 2009. The CPSU also supported extending the procedural safeguards in the *Public Service Act* to persons other than APS employees: Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

70 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

14.49 APRA submitted that s 48AC of the APRA Act already sets out processes for dealing with suspected misconduct. APRA did not support the development of separate processes for dealing with conduct relating to breach of secrecy provisions.<sup>71</sup> The AFP advised that it has in place a robust framework for detecting, investigating and dealing with breaches of secrecy laws by AFP appointees.<sup>72</sup>

### **ALRC's views**

14.50 An overarching theme of this Discussion Paper is that—except in the most serious cases—the unauthorised disclosure of Commonwealth information should generally be dealt with through administrative disciplinary proceedings, rather than through the criminal law. It is therefore important to ensure that a sound administrative secrecy regime is in place for all Commonwealth employees—not only APS employees. A just and effective administrative regime involves consideration not only of the conduct regulated by the secrecy obligation, but also of the procedural framework through which an Australian Government agency deals with breaches, and suspected breaches, of the obligation.

#### ***Framing administrative secrecy requirements***

14.51 What obligations of secrecy should apply to Commonwealth employees who are not employed under the *Public Service Act*?

14.52 In Chapter 13, the ALRC proposes that the duty of non-disclosure that governs APS employees should apply to information that has come to the employee's knowledge or possession by reason of his or her being an APS employee, where the disclosure is reasonably likely to be prejudicial to the effective working of government.<sup>73</sup>

14.53 Many Commonwealth employees that are not employed under the *Public Service Act* perform substantially similar duties to APS employees. Whether or not the person is employed under the *Public Service Act* does not necessarily depend on considerations of duties of confidentiality and non-disclosure, but may be based on other considerations, such as labour market forces. The ALRC considers that the obligation of non-disclosure set out in reg 2.1 of the *Public Service Regulations* should apply to these employees. This will ensure, in the administrative setting, that there is ‘a consistent approach across government to the protection of Commonwealth information’—a key objective in the Terms of Reference for this Inquiry.<sup>74</sup>

---

<sup>71</sup> Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009. See also N Rogers, *Submission SR 01*, 9 December 2008. The AGD also noted that procedural safeguards in the *Public Service Act* operate more broadly than just breaches of secrecy provisions: Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

<sup>72</sup> Australian Federal Police, *Submission SR 33*, 3 March 2009.

<sup>73</sup> Proposal 13–1.

<sup>74</sup> The Terms of Reference are set out at the beginning of this Discussion Paper.

14.54 The appropriateness of equivalent administrative secrecy obligations for employees inside and outside the APS is illustrated by those statutory authorities that employ staff under both the *Public Service Act* and their enabling legislation. The ALRC acknowledges the advice from ASIC (one such authority) that the staff that it employs other than under the *Public Service Act* are nevertheless required to comply with the APS Code of Conduct. Other statutory authorities—for example, the Australian Institute of Criminology and the ALRC itself—have voluntarily taken on the APS Code of Conduct as the template for their employee conduct requirements.

14.55 The ALRC considers that reg 2.1 could be adopted as the administrative secrecy requirement for a particular class of Commonwealth employees even where the entire APS Code of Conduct should not apply. For example, some of the conduct requirements in the Parliamentary Service Code of Conduct differ from those that apply to the APS because of the political environment within which parliamentary departments operate. However, the ALRC is not aware of any rationale to justify the minor differences between reg 2.1 and the administrative secrecy requirements that currently apply to employees of parliamentary departments and ministerial staff employed under the MOPS Act.

14.56 In some situations, however, the duties of a Commonwealth employee may be sufficiently different from those in the APS to warrant distinct administrative secrecy obligations. For example, it has been argued that, for the ADF to function effectively, members must work within a very different disciplinary regime from that which applies elsewhere in the public service. As one stakeholder submitted to the Senate Foreign Affairs Defence and Trade References Committee inquiry into the effectiveness of Australia's military justice system:

a democracy cannot maintain an effective Defence Force without that force being subject to a code of disciplinary legislation that specifically covers the purposes, situations, conditions and exigencies of war. No extension of civil codes of law can, or necessarily should, meet those requirements.<sup>75</sup>

14.57 The duties of a Commonwealth employee also might not easily translate to the APS framework for an individual (other than a ministerial staffer) employed under the MOPS Act. These employees work for the legislative, rather than the executive, arm of government. This may result in a different relationship with Commonwealth information which may justify a different secrecy obligation. The secrecy obligations that apply to employees of statutory authorities that perform a predominantly commercial role might also warrant separate consideration.

14.58 The above examples do not represent the concluded views of the ALRC on the administrative secrecy obligations that should apply to specific Commonwealth

---

<sup>75</sup> Parliament of Australia—Senate Foreign Affairs Defence and Trade References Committee, *The Effectiveness of Australia's Military Justice System* (2005), [2.10], citing the submission of Mr Neil James of the Australian Defence Association.

employees. Rather, they are intended to illustrate the ALRC's current thinking about how the Australian Government should determine whether or not a Commonwealth employment relationship should be governed by equivalent secrecy requirements to those that apply to the APS.

#### ***Processes for investigation and enforcement***

14.59 As noted above, the *Public Service Act* and related instruments provide high-level procedural safeguards for the investigation and determination of suspected breaches of secrecy provisions. These reflect general administrative law principles,<sup>76</sup> including requirements that:

- the procedure for determining whether any Australian Government employee has breached an administrative secrecy provision has 'due regard to procedural fairness';<sup>77</sup>
- employees are given information, and a reasonable opportunity to make a statement, before a determination of breach is made;<sup>78</sup>
- processes for determining breaches are carried out informally and expeditiously,<sup>79</sup> and
- a person who determines whether an employee has breached an administrative secrecy requirement is, and appears to be, independent and unbiased.<sup>80</sup>

14.60 These obligations are likely to be appropriate for the vast majority of Australian Government employment situations. In limited circumstances, however, particular features of the employing agency may warrant a different approach.

14.61 For example, the *Public Service Act* includes a mechanism for merits review of Code of Conduct determinations. Depending on the structure of the employing agency, providing for an independent merits review may not be feasible. In other situations, the functions of the agency, and the nature of the employment duties, may justify departure from procedures required under the *Public Service Act*.

14.62 For example, the heightened difficulty of investigating misconduct in the context of law enforcement, and the special position of trust that is accorded to law enforcement officers, may justify some variations from the procedural safeguards set

---

<sup>76</sup> See, eg, R Douglas and M Jones, *Administrative Law: Commentary and Materials* (3rd ed, 1999).

<sup>77</sup> *Public Service Act 1999* (Cth) s 15(3).

<sup>78</sup> *Public Service Commissioner's Directions 1999* (Cth) cl 5.2.

<sup>79</sup> *Ibid* cl 5.3.

<sup>80</sup> *Ibid* cl 5.4. The Commissioner's Directions also require a written record to be prepared noting the outcome of the investigation: cl 5.5.

out in the *Public Service Act*. In the report, *Integrity: But Not by Trust Alone*, the ALRC noted the special difficulties in investigating police misconduct:

- police know the system and are likely to have early warning of any interest in their activities
- they are skilled in investigation techniques and counter surveillance
- they are likely to have corrupt associates willing to cover for them
- they are experienced in being interviewed, in being cross examined and in giving evidence
- their good credibility and character are readily assumed by jurors, courts and tribunals
- they can exert considerable personal influence over internal informants and internal investigators particularly if they hold senior rank.<sup>81</sup>

14.63 What, if any, variations will be warranted should be considered by the Australian Government on an agency-by-agency basis.

**Proposal 14–1** Australian Government agencies that employ persons other than under the *Public Service Act 1999* (Cth)—including agencies prescribed under the *Financial Management and Accountability Act 1997* (Cth) and bodies subject to the *Commonwealth Authorities and Companies Act 1997* (Cth)—should:

- (a) include in the agency’s terms and conditions of employment the requirements set out in reg 2.1 of the *Public Service Regulations 1999* (Cth), to the extent that these requirements are consistent with the agency’s functions and structure; and
- (b) adopt the safeguards set out in the *Public Service Act* for dealing with suspected breaches of reg 2.1, to the extent that these safeguards are consistent with the agency’s functions and structure.

## Former Commonwealth employees

14.64 Administrative disciplinary penalties only apply to current Commonwealth employees. They do not apply, for example, to a person whose employment has terminated prior to the disclosure of secret information, or who has resigned when an

<sup>81</sup> Australian Law Reform Commission, *Integrity: But Not by Trust Alone: AFP & NCA Complaints and Disciplinary Systems*, ALRC 82 (1996), [9.141]. These factors had been identified in the interim report of the Royal Commission into the NSW Police Service.

investigation into that person's conduct commenced. How, therefore, can official information held by former Commonwealth employees best be protected?

14.65 The equitable duty of confidence provides some protection for information in the hands of former employees. As discussed in Chapter 5, this duty restricts an employee from using or disclosing certain confidential information obtained during the course of employment. In the case of *Commonwealth v Fairfax*, Mason J commented that, in the context of government information, disclosure would be restrained where this would be 'inimical to the public interest because national security, relations with foreign countries or the ordinary course of business of government will be prejudiced'.<sup>82</sup>

14.66 In the case of *Faccenda Chicken Ltd v Fowler*, Neill LJ of the Civil Division of the Court of Appeal of England and Wales set out the law, as it applies to former employees, as follows:

The implied term which imposes an obligation on the employee as to his conduct after the determination of the employment is more restricted in its scope than that which imposes a general duty of good faith. It is clear that the obligation not to use or disclose information may cover secret processes of manufacture ... or designs or special methods of construction ... and other information which is of a sufficiently high degree of confidentiality as to amount to a trade secret.

The obligation does not extend, however, to cover all information which is given to or acquired by the employee while in his employment, and in particular may not cover information which is only 'confidential' in the sense that an unauthorised disclosure of such information to a third party while the employment subsisted would be a clear breach of the duty of good faith.<sup>83</sup>

14.67 Neill LJ then considered the factors that should be taken into account in determining whether a particular item of information falls within a former employee's duty of confidentiality:

(a) *The nature of the employment.* Thus employment in a capacity where 'confidential' material is habitually handled may impose a high obligation of confidentiality because the employee can be expected to realise its sensitive nature to a greater extent than if he were employed in a capacity where such material reaches him only occasionally or incidentally. (b) *The nature of the information itself.* In our judgment the information will only be protected if it can properly be classed as a trade secret or as material which, while not properly to be described as a trade secret, is in all the circumstances of such a highly confidential nature as to require the same protection as a trade secret *eo nomine*.<sup>84</sup>

---

82      *Commonwealth v Fairfax* (1980) 147 CLR 39, 52.

83      *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 625.

84      *Ibid*, 626 (emphasis added).

14.68 Although the court considered that it was ‘clearly impossible’ to provide a list of matters that would qualify as trade secrets or their equivalent, a relevant factor was the restriction of the circulation of information to a limited number of people.<sup>85</sup> Whether the employer ‘impressed on the employee the confidentiality of the information’ will also be significant.<sup>86</sup>

14.69 The question of what would qualify as a ‘trade secret’ or equivalent in the context of information in the possession of a former government employee has not been the subject of judicial consideration in Australia or elsewhere.

### Submissions and consultations

14.70 In IP 34, the ALRC asked in what circumstances should secrecy provisions regulate former Commonwealth officers and others who have left positions subject to secrecy provisions.<sup>87</sup> The submissions on IP 34 that addressed this issue are discussed in detail in Chapter 7, in the context of the general secrecy offence.

14.71 As noted in that chapter, there was widespread support among government and other stakeholders for applying secrecy provisions to former Commonwealth employees.<sup>88</sup> The submissions of the AGD and the Treasury, for example, pointed to the potential for the purpose of provisions aimed at protecting sensitive information to be frustrated simply by a person leaving the service of the Australian Government.<sup>89</sup> The Department of Human Services (DHS) noted that the period after a person leaves Australian Government employment is ‘a period of increased risk of disclosure, since they are no longer under the watchful eye or normative influence of the employing agency’.<sup>90</sup>

14.72 Although ASIC supported the application of secrecy provisions to former Commonwealth officers, it submitted that it ‘may be improper to impose the same secrecy obligations on a former Commonwealth officer as are imposed on current officers’. Accordingly, a former officer’s obligations of non-disclosure should be limited ‘to the extent that they will continue to protect information that, if disclosed,

---

85 Ibid, 627.

86 Ibid.

87 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–3.

88 See, eg, Australian Intelligence Community, *Submission SR 37*, 6 March 2009; NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009; Australian Federal Police, *Submission SR 33*, 3 March 2009; Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

89 Attorney-General’s Department, *Submission SR 36*, 6 March 2009; The Treasury, *Submission SR 22*, 19 February 2009.

90 Department of Human Services, *Submission SR 26*, 20 February 2009.

could injure the private and public interests that the secrecy provisions were designed to protect'.<sup>91</sup>

14.73 PIAC submitted that the equitable duty of confidence provided an appropriate level of protection for government information held by former Commonwealth officers.<sup>92</sup>

### **ALRC's views**

14.74 In some circumstances, the time when a Commonwealth employee leaves his or her employment will be associated with a risk of the unauthorised disclosure of official information. It is possible, for example, that an employee's resignation will be associated with an ongoing grievance with the agency, or other employees of the agency, for which vindication is sought. Even where no such dispute has occurred, the fact that a former employee is no longer under the direct control or influence of the employing agency may provide a greater opportunity to disclose Commonwealth information and fewer inhibitions not to disclose. Therefore, there should be some way of protecting official information in the hands of former employees.

14.75 In the ALRC's view, however, it is not feasible to impose ongoing administrative secrecy obligations on those who leave Commonwealth employment. The ability of an agency head to impose administrative penalties arises out of the statutory nature of the employment relationship. In the case of a former employee, this relationship clearly no longer exists. Further, the penalties that may be imposed under administrative disciplinary regimes have little, if any, practical application to persons that are not in an ongoing employment relationship with the Commonwealth. Of the administrative penalties that an agency head may impose for breach of the APS Code of Conduct, for example, only a fine has the potential to translate to the context of former employees. Even here, the quantum of the fine is determined with reference to the employee's salary.<sup>93</sup>

14.76 In Chapter 8, the ALRC expresses the view that the proposed general secrecy offence should encompass former Commonwealth employees. This will serve as a valuable deterrent for a former employee who is considering disclosing information.<sup>94</sup> In some situations, a specific secrecy offence may also apply to the unauthorised disclosure of information by a former Commonwealth employee.<sup>95</sup>

14.77 The equitable duty of confidence continues to apply to an employee when he or she is no longer in an employment relationship—albeit in a more limited manner. The

---

91 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

92 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

93 Penalties for breach of the APS Code of Conduct are discussed in Ch 13.

94 As discussed in Ch 7, the proposed general criminal offence will apply where a disclosure would be reasonably likely to cause harm to certain specified public interests including, eg, the security, defence or international relations of the Commonwealth: Proposal 7–1.

95 Specific secrecy offences are discussed in Chs 10–12.

issue of what government information will qualify as a ‘trade secret’ or information which ‘is in all the circumstances of such a highly confidential nature as to require the same protection as a trade secret’ remains open for judicial determination.<sup>96</sup> However, this will depend on the extent to which the employee can be expected to realise the information’s sensitivity, including the number of people that had access to the information and the degree to which the employing agency impressed the confidential nature of the information on the former employee. Under these criteria, for example, security classified information (which has a limited circulation and clear indication of confidentiality) may well be caught by an ongoing equitable duty.

14.78 For criminal secrecy offences and the equitable duty of confidence to satisfy the objective of deterrence, however, the ongoing nature of these laws must be made clear to employees at the time of separation. The ALRC proposes, therefore, that Australian Government agencies should remind their employees, on termination, of the employee’s continuing legal responsibilities. This could be done, for example, during an employee’s exit interview. This reminder is also an opportunity for agencies to reinforce the personal nature of non-disclosure obligations, as discussed in the context of contracted service providers, below.

**Proposal 14–2** Australian Government agencies should remind employees, on termination, of their continuing liability under the general secrecy offence and any relevant specific secrecy offence, and of their obligations under the equitable duty of confidence.

## Persons outside Commonwealth employment

14.79 In the following section, the ALRC considers the responsibilities of non-disclosure placed upon individuals who have access to Commonwealth information for reasons other than an employment relationship. These include:

- private-sector employees who access Commonwealth information under a contract for services;
- members of Commonwealth boards and committees;
- state and territory public sector employees; and
- individuals without any clear relationship to the Commonwealth.

<sup>96</sup> *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 626. As discussed in Ch 5, the *Fairfax* case shows that there is a high threshold before the equitable action will arise in the context of government information: *Commonwealth v Fairfax* (1980) 147 CLR 39.

## **Contracted service providers**

### ***Background***

14.80 The Commonwealth outsources a wide variety of functions to contracted service providers. In the 2007–08 financial year, Australian Government agencies reported the award of almost 70,000 contracts and standing offer arrangements with a value of \$10,000 or more—amounting to a combined value of approximately \$26.4 billion.<sup>97</sup> Many of these contracts are with private sector service providers.<sup>98</sup>

14.81 Depending on the services being rendered, a contracted service provider could be given access to extensive and/or highly sensitive Commonwealth information. Hypothetically, for example, a contracted service provider could be asked to determine how resources should be allocated among various aged-care facilities. To carry out this task, the contracted service provider may need the agency to provide information as wide-ranging as budget estimates for the facilities, the current rate of use of each of the facilities, demographic details of the people who have used them, and the reasons for use. A further illustration of the sensitive nature of information that may be released to private sector contractors can be drawn from an article in *The Canberra Times* in April 2009, reporting that staff of a company, outsourced by the Australian Taxation Office to conduct its call centre work, could gain access to private income tax records. In particular, the article raised concerns that access was not conditional on the obligation ‘to comply with the strict code of behaviour imposed on public servants’.<sup>99</sup>

14.82 In other situations, the information warranting protection may be generated by the contracted service provider itself. This can be illustrated in the context of contractors responsible for providing immigration detention services, and sub-contractors responsible for providing health services, to detainees of the (now closed) Baxter Detention Centre.<sup>100</sup> These service providers had the responsibility of gathering highly sensitive information about the operation of a government facility.

14.83 Since persons engaged by contracted service providers are not in an employment relationship with the Commonwealth, administrative penalties do not apply to their information-handling practices. Accordingly, the principal mechanism of controlling the flow of Commonwealth information is contractual.

---

97 Department of Finance and Deregulation, *Statistics on Australian Government Procurement Contracts* (2009) <<http://www.finance.gov.au/publications/statistics-on-commonwealth-purchasing-contracts/index.html>> at 15 April 2009. Agencies subject to the FMA Act are required by the *Commonwealth Procurement Guidelines* to publish standing offer arrangements and contracts with a value of \$10,000 or more, to demonstrate openness, transparency and accountability for procurement decisions. From 1 January 2005, CAC Act bodies subject to the *CAC Act Procurement Directions* are also required to publish details of certain contracts and standing offers.

98 Other than the private sector, the Australian Government may also enter into contracts with Commonwealth statutory entities and state and territory departments and entities.

99 M Mannheim, ‘Concern over Access to Tax Records’, *The Canberra Times* (Canberra), 27 April 2009, 3. A description of the contractual and subcontractual arrangements for service provision at the Baxter Detention Centre is set out in *S v Secretary, Department of Immigration and Multicultural and Indigenous Affairs* (2005) 143 FCR 217.

14.84 In addition to—or in the absence of—a contractual relationship, an equitable duty of confidence may be enlivened where a contractor has accessed Commonwealth information that is inherently confidential and imparted in circumstances of confidentiality.

#### ***Guidance on Confidentiality in Procurement (FMG 3)***

14.85 The Department of Finance and Administration (now the Department of Finance and Deregulation) has issued *Financial Management Guidance No 3—Guidance on Confidentiality in Procurement* (FMG 3). The FMG 3 provides general advice on managing confidential information in contracted relationships as well as model confidentiality clauses for Australian Government agencies to include in contracts that they enter into.

#### ***Confidential information***

14.86 The FMG 3 advises that ‘confidential information’ comprises information that is either:

- required to be kept confidential due to the operation of legislation; or
- determined by an agency to be confidential.<sup>101</sup>

14.87 Legislative requirements to keep information confidential include, for example, information within the scope of a secrecy provision and information governed by the *Privacy Act 1988* (Cth). Where there is no legislative requirement to maintain confidentiality, an agency may make a determination that information held by the Australian Government or a contracted service provider should be treated as confidential.

14.88 An Australian Government agency does not have unlimited discretion to designate what information under a contract is confidential. The Australian Government Solicitor (AGS) has advised that:

There are limits on the kind of information which can be protected as confidential under a contract. For example, if an attempt is made to protect from disclosure certain Government Information<sup>102</sup> as confidential information when an analysis of public interest issues leads to a conclusion that the information is not confidential in nature ('inherently confidential'), a court may refuse to enforce a contractual obligation not to disclose that information.<sup>103</sup>

---

101 Australian Government Department of Finance and Administration, *Financial Management Guidance No 3: Guidance on Confidentiality in Procurement*, 1 July 2007, [3.1].

102 Government Information in this context is defined as ‘information about government which has been generated by government’: Australian Government Solicitor, *Legal Briefing No 64: Identifying and Protecting Confidential Information* (2002).

103 Ibid. The AGS goes on to consider the circumstances in which an equitable obligation to protect information arises in the absence of a contract.

14.89 The FMG 3 suggests that it may be appropriate for an Australian Government agency to determine that information should be treated as confidential under a contract where:

- disclosure would be contrary to the public interest—for example, because it could compromise national security or defence or disclose Cabinet deliberations;
- the Australian Government holds intellectual property rights over the information; or
- the contracted service provider demonstrates that the commercial sensitivity of the information warrants confidentiality.<sup>104</sup>

14.90 Where an agency has determined that information must be kept confidential, it will usually protect this information by including a specific confidentiality clause in the contract. Clauses can protect the confidentiality of all or part of the contract itself; or information obtained or generated in performing the contract.<sup>105</sup> The FMG 3 suggests that a specific confidentiality clause could be used, for example, where ‘the contract is for a consultant to prepare a confidential report which is expected to deal with sensitive public interests’.<sup>106</sup>

#### ***Confidential Commonwealth information***

14.91 Not all confidential information under a contract for services is under the control of the Commonwealth. For example, trade secret information that a private sector partner provides to an Australian Government agency is likely to be confidential information the use and disclosure of which is under the control of the contracting partner. The question, therefore, is when will ‘confidential information’ also be ‘confidential Commonwealth information’?

14.92 The model confidentiality clause set out in the FMG 3 provides that ‘a Party must not, without the prior written consent of the other Party, disclose any Confidential Information of the other Party to a third party’.<sup>107</sup> The FMG 3 does not specify what information will be ‘of the other Party’.

---

104 Australian Government Department of Finance and Administration, *Financial Management Guidance No 3: Guidance on Confidentiality in Procurement*, 1 July 2007, [3.9]–[3.14]. The four criteria that must be met for a contracted service provider’s commercial information to be kept confidential are the information to be protected is specifically identified; the information must be commercially sensitive and therefore not generally known or ascertainable; disclosure would cause unreasonable detriment to the owner of the information or another party; and the information was provided under an understanding that it would remain confidential: [3.15]–[3.22].

105 Ibid, [5.6].

106 Ibid, [5.9].

107 Ibid, Appendix 3, cl B3(1) (emphasis added).

14.93 One guide to when information will be ‘Commonwealth information’ is the definition of ‘official information’ in the *Australian Government Protective Security Manual* (PSM)—that is, ‘any information that is developed, received or collected by or on behalf of the Commonwealth Government, through its agencies and contractors’.<sup>108</sup> Unless Commonwealth ownership of information is expressly identified in the contract, however, the courts will determine the question of whether information is ‘of the Commonwealth’ in accordance with general principles for interpreting express contractual terms. This is a pragmatic judgment, involving

the ascertainment of the meaning which the document would convey to a reasonable person having all the background knowledge which would reasonably have been available to the parties in the situation in which they were at the time of the contract.<sup>109</sup>

#### ***Exceptions to the obligation of confidentiality***

14.94 The model confidentiality clause in FMG 3 sets out exceptions to the obligation of non-disclosure, where information is:

- disclosed to a party’s advisers or employees in order to comply with obligations, or to exercise rights, under the contract;
- disclosed to a party’s internal management personnel to enable effective management or auditing of contract-related activities;
- authorised or required by law to be disclosed; or
- otherwise in the public domain.<sup>110</sup>

#### ***Binding individual employees***

14.95 As noted by the AGS,

An organisation’s employees are not a party to any confidentiality agreement that the organisation may enter into with the agency. The same goes for subcontractors and the employees of subcontractors as well as the employees of subsidiary and holding companies for the commercialisation partner. The contract itself would not be able to impose any direct penalty on the employees for releasing confidential ... information belonging to the agency.<sup>111</sup>

---

108 Australian Government Attorney-General’s Department, *Australian Government Protective Security Manual (PSM)* (2005), pt C, [1.3].

109 N Seddon and M Ellinghaus, *Cheshire and Fifoot’s Law of Contract* (8th ed, 2002), [10.31], citing *Maggbury Pty Ltd v Hafele Australia Pty Ltd* (2001) 210 CLR 181, [11]. This phrase was originally stated by Lord Hoffman in *Investors Compensation Scheme Ltd v West Bromwich Building Society* [1998] 1 All ER 98, 114.

110 Exceptions also apply to permit the Commonwealth to disclose information to the responsible minister, a House or Committee of Parliament or shared within the Commonwealth to serve legitimate interests.

111 A Snooks, *Commercial Notes No. 25: Protecting Commonwealth Information* (2008).

14.96 Accordingly, where an agency wishes to ensure greater protection for confidential information, it may enter into confidentiality arrangements with nominated personnel of the contracted service provider, including subcontractors and their personnel.

The purpose of entering into these arrangements with nominated personnel is not primarily so the agency can take direct action against or sue individuals (as this is highly unlikely in practice) but, rather, to act as a clear reminder to those individuals of their responsibilities to protect the confidentiality of the agency's intellectual property that they may see. This method can be highly effective when used in conjunction with a confidentiality agreement with the commercialisation partner. The element of personal responsibility that is missing from the agreement with the partner is provided through the agreements with the individuals.<sup>112</sup>

14.97 In addition to a requirement for the contracted service provider to arrange for the provision of confidentiality undertakings from its personnel, confidentiality agreements could require a contracted service provider to:

- limit the release of Commonwealth confidential information on a 'need to know' basis—for example, by requiring the provider to provide a list of personnel who may gain access to the information, for the agency's approval; or
- ensure that its nominated personnel have been informed of the confidential information that requires protection, or trained in how to use the information in compliance with the agreement.<sup>113</sup>

14.98 The model confidentiality clause set out in the FMG 3 provides the option for an agency to require a contracting party to obtain written undertakings from individuals (other than Commonwealth employees) who have access to confidential Commonwealth information about the use and disclosure of the information. Inclusion of a requirement for written undertakings is optional. The FMG 3 suggests that an undertaking is likely to be relevant

when the Commonwealth is seeking to obtain the maximum protection for sensitive Commonwealth information or when the Commonwealth intends to disclose confidential information to third party consultants.<sup>114</sup>

14.99 The equitable duty of confidence may also restrain individuals who receive confidential Commonwealth information in accordance with a contract for services from disclosing the information without authorisation. As discussed in Chapter 5, equity may provide a remedy for the unauthorised use of confidential information

<sup>112</sup> Ibid.

<sup>113</sup> Ibid. The AGS notes, however, that private sector organisations may resist having confidentiality undertakings imposed on their personnel—for example, because they are of the view that these people are already sufficiently bound by confidentiality obligations.

<sup>114</sup> Australian Government Department of Finance and Administration, *Financial Management Guidance No 3: Guidance on Confidentiality in Procurement*, 1 July 2007, 39.

which has been imparted in circumstances importing an obligation of confidence. This obligation is independent of any contractual or employment relationship—although the confidential nature of the information may derive from the terms of the contract.

14.100 In some circumstances, the proposed general secrecy offence will apply to a person who discloses Commonwealth information that he or she obtained under a contract for services.<sup>115</sup> Specific secrecy offences also may be relevant.<sup>116</sup>

#### *Applying the APS Code of Conduct*

14.101 Another option for imposing secrecy obligations on the personnel of contracted service providers is to include a contractual requirement that some, or all, of those who have access to information must comply with the APS Code of Conduct or some other administrative secrecy template. This is similar to the approach that has been taken, for example, in the *Code of Conduct for Victorian Public Sector Employees*:

Public sector employers are to require contractors or consultants engaged in or by their public body (including contractors or consultants engaged through an employment agency) to comply with this Code of Conduct and relevant policies and procedures, where the contractors or consultants:

- supervise public sector employees;
- undertake work that is of a similar nature to the work undertaken by public sector employees at a premise or location generally regarded as a public sector workplace; and
- use or have access to public sector resources or information that are not normally accessible or available to the public.<sup>117</sup>

#### *Submissions and consultations*

14.102 In IP 34, the ALRC asked in what circumstances should secrecy provisions regulate the behaviour of persons other than Commonwealth officers, such as consultants and others who provide goods and services to the Australian Government and those who enter into arrangements with the Australian Government.<sup>118</sup>

14.103 Australian Government agencies expressed broad support for applying secrecy laws to consultants and contracted service providers. APRA, for example, submitted that it may be appropriate for a secrecy provision to apply to:

IT consultants who, in the process of providing IT services, have access to protected information or documents in APRA's computer systems; consultants retained to provide assistance in investigations, eg forensic accountants; professional advisers;

---

115 The elements of the proposed general secrecy offence are discussed in detail in Ch 8.

116 Specific secrecy offences are discussed in Chs 10–12.

117 Victorian Government State Services Authority, *Code of Conduct for Victorian Public Sector Employees* (2007) <<http://www.ssa.vic.gov.au/>> at 6 March 2009, [1.4].

118 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–1. This question was not specifically directed to the administrative context.

secondees from other regulators; temporary staff supplied by agencies (who are employed by the agency rather than APRA); and persons retained as, or working for, external administrators (eg an [authorised deposit-taking institution] statutory manager appointed under the *Banking Act 1959*).<sup>119</sup>

14.104 The Treasury expressed the view that it was appropriate for secrecy obligations to have a wide application to reflect the increasing use of private individuals and entities to assist in the provision of government services.<sup>120</sup> The New South Wales (NSW) Young Lawyers Human Rights Committee agreed that all people who handle government information should be subject to secrecy laws, including any person or organisation hired by the Australian Government to perform work on its behalf.<sup>121</sup>

14.105 The CPSU recommended that secrecy provisions, along with associated statutory exceptions and ‘protected disclosure’ legislation, should apply to private sector consultants and companies who do business with government as well as other Australian Government entities.<sup>122</sup> ASIC agreed that secrecy provisions should regulate anyone who provides goods and services to the Commonwealth, such as contractors, regardless of the arrangements under which they are engaged to provide those goods and services.<sup>123</sup>

14.106 The DHS noted the important role that secrecy provisions play in imparting a level of personal responsibility to staff. The DHS advised of the importance of contracted staff and staff of contracted service providers appreciating the personal nature of their secrecy obligations.<sup>124</sup>

14.107 On the other hand, Australia’s Right to Know coalition submitted that:

Confidentiality provisions in contracts should only cover material which is truly confidential, such as a trade secret. The terms of an agreement between a commercial entity and the government will not normally be entirely confidential, and often the terms and desirability of such contracts should be subject to public scrutiny. This is especially the case for contracts involving the sale of or provision of public facilities, infrastructure or services.

---

119 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009. See also Australian Federal Police, *Submission SR 33*, 3 March 2009; Department of Climate Change, *Submission SR 27*, 23 February 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; Confidential, *Submission SR 21*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009.

120 The Treasury, *Submission SR 22*, 19 February 2009.

121 NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009. PIAC agreed that persons who contract with or act as consultants to the government should be regulated by the same set of secrecy provisions that govern the agency or Commonwealth officers with which they are dealing: Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

122 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

123 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

124 Department of Human Services, *Submission SR 26*, 20 February 2009.

Many recent contracts impose a general obligation of confidentiality over material that is not truly confidential so that there is a contractual obligation not to reveal the information. This device should not be permitted or condoned in either government departments or in bodies established or funded by government, privately contracted government services and government-subsidised private sector bodies.<sup>125</sup>

#### *ALRC's views*

14.108 Contractual confidentiality provisions are a valuable tool for protecting Commonwealth information that is disclosed to, or generated by, private sector contracted service providers and subcontractors. Clearly drafted confidentiality clauses provide certainty to contracted service providers as to the manner in which they should deal with particular Commonwealth information. Such service providers may be sued for breach of contract for inappropriate disclosures, or restrained from disclosing inappropriately in an action for breach of confidence.

14.109 However, contractual requirements only apply to the contracting organisation itself—no obligations are directly imposed on employees who deal with the information.

14.110 Where an employee of a contracting organisation wrongly discloses confidential Commonwealth information—thereby leaving the organisation open to an action in breach of contract—it is for the employing organisation to take steps independently to discipline that employee. However, the ALRC agrees with the DHS about the value of impressing upon employees their personal responsibilities for protecting information received under a contract with the Australian Government. The ALRC proposes that Australian Government agencies should require contracting organisations to ask employees who receive or generate confidential information under the contract to agree to comply with the confidentiality requirements.

14.111 At this stage, the ALRC has not specified the way in which this agreement must be sought. In the ALRC's view it will normally be appropriate for the contracting organisation to decide how it will assure itself of the compliance of its personnel. In some circumstances, however, the potential consequences of disclosure of Commonwealth information will warrant an Australian Government agency requesting the contracted service provider to arrange for subcontractors, employees, and others to provide a signed deed of confidentiality.<sup>126</sup> The option to require such a deed is already made clear in the FMG 3 and, therefore, is not the subject of an ALRC proposal.

14.112 In Chapter 15, the ALRC further considers the responsibility of private sector organisations that perform services for or on behalf of the Australian Government to make employees who have access to Commonwealth information aware of their obligations of secrecy, including the circumstances in which liability

---

125 Australia's Right to Know, *Submission SR 35*, 6 March 2009.

126 See, eg, the discussion of the deed of confidentiality for the Trusted Information Sharing Network in Ch 3.

could result.<sup>127</sup> These obligations may include the equitable duty of confidentiality and the general secrecy offence, in addition to contractual confidentiality requirements.

14.113 The model exceptions to the obligation of non-disclosure set out in the FMG 3 allow the necessary flexibility for a contracted service provider to perform its functions effectively. The ALRC proposes that confidentiality clauses should also include an exception for conduct that amounts to a public interest disclosure under public interest disclosure legislation. This is consistent with the recommendation of the House of Representatives Standing Committee on Legal and Constitutional Affairs, in its report on whistleblowing in the Commonwealth public sector, that people who are entitled to make a protected disclosure should include contractors and consultants engaged by the public sector and their employees.<sup>128</sup>

14.114 The ALRC is not proposing that contracts for services should include, as a matter of course, a requirement for personnel to comply with the APS Code of Conduct. The Australian Government enters into contracts in a wide variety of circumstances. In many of these situations it is unsuitable to impose on contracting personnel a duty of non-disclosure ‘where the disclosure is reasonably likely to be prejudicial to the effective working of government’.<sup>129</sup> For example, where a contract involves access only to limited Commonwealth information, it normally will be clearer to identify the precise information that is the subject of protection. Even where a contract sets out a broader relationship between the Australian Government and a private sector provider, it may be unreasonable to expect personnel of that provider to ascertain the circumstances when disclosure of information is likely to be prejudicial to the government. Commonwealth information can be sufficiently protected by requiring personnel to comply with the contractual confidentiality clause.

**Proposal 14–3** An Australian Government agency that enters into a contract for services involving access to Commonwealth information should include in the contract a confidentiality clause that:

- (a) clearly sets out the categories of information that are confidential Commonwealth information;
- (b) requires persons (other than Commonwealth employees) who have access to confidential Commonwealth information by reason of the contract to agree to comply with the contractual confidentiality requirements; and

127 Proposal 15–7.

128 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 3.

129 The duty of non-disclosure in the APS Code of Conduct is discussed in detail in Ch 13.

- (c) permits the disclosure of confidential Commonwealth information where the disclosure amounts to a public interest disclosure under proposed Commonwealth public interest disclosure legislation.

## Members of boards and committees

14.115 The various roles of government boards and committees have been explained as follows:

**Governing Boards** are empowered to govern the management of the organisation which are subject to control and direction of the Minister but the circumstances in which ministerial control and direction are exercised are specific.

**Advisory Boards** provide advice to a portfolio Minister on matters relevant to the management of an authority but the Minister retains unfettered right to control and direct the Board and the [Chief Executive Officer].

**Advisory Committees, Councils etc** provide advice on policy or operational issues with little or no policy determination or operational executive functions.<sup>130</sup>

14.116 Depending on the functions of a Commonwealth board or committee, and the context in which it operates, members may handle highly sensitive information. Advisory committees and councils, for example, typically perform a deliberative function for an Australian Government agency or minister. As part of this role, committee members may be privy to internal policy discussions, unauthorised disclosure of which could cause harm to the implementation of government policies or programs. In other situations, members may come into possession of information that requires protection because it is personal or commercially-sensitive information. For example, sponsors of pharmaceuticals that are seeking to have a product added to the Pharmaceutical Benefits Scheme (PBS) must provide members of the Pharmaceutical Benefits Advisory Committee (PBAC) with extensive commercial information. This includes, for example, a comparison between the clinical benefits of the product and other similar pharmaceuticals (including information from any unpublished studies) and an evaluation of the economic implications of listing the product on the PBS.<sup>131</sup>

14.117 The terms and conditions of appointment of members of boards and committees directly established under legislation are usually at the discretion of the Governor-General or responsible minister. The establishing legislation, however, often

---

130 New South Wales Premier's Department, *Conduct Guidelines for Members of NSW Government Boards and Committees* (2001), 2. Although this description was in the context of the NSW Government, the same definitions apply in the context of the Australian Government.

131 Department of Health and Ageing, *1995 Guidelines for the Pharmaceutical Industry on Preparation of Submissions to the PBAC* (2004) <<http://www.health.gov.au/internet/main/publishing.nsf/Content/health-pbs-general-pubs-pharmpac-gusubpac.htm>> at 21 April 2009.

provides for the prospect of termination of membership in the event of ‘misbehaviour’.<sup>132</sup>

14.118 The terms and conditions of appointment of members of advisory committees or councils without an express legislative foundation may be determined by the responsible minister or agency. The conduct requirements that apply to members of Commonwealth boards and committees are not usually publicly available.

#### *ALRC’s views*

14.119 Members of Commonwealth boards and committees will often have access to sensitive information. It is important, therefore, to make sure that these members are subject to sufficient requirements of confidentiality. A logical place for these to be located is in the terms and conditions of appointment. However, what level of confidentiality should be imposed on members of boards and committees?

14.120 In this Discussion Paper, the ALRC proposes that APS employees, and most other Commonwealth employees, should be under a duty not to disclose information that has come to their knowledge or into their possession by reason of being an APS employee, where the disclosure is reasonably likely to be prejudicial to the effective working of government. In certain situations, the structure and function of an employing agency will warrant the imposition of some other administrative secrecy requirement.<sup>133</sup>

14.121 In the ALRC’s preliminary view, it is reasonable to impose equivalent secrecy requirements on members of boards and committees to those that apply in a related Commonwealth employment context—in particular, a Commonwealth employee who accesses similar information to the board or committee. For example, members of PBAC, discussed above, could be made subject to equivalent secrecy obligations to those that apply to employees of the Therapeutic Goods Administration, who provide the secretariat for PBAC.

14.122 Often this will mean that members of boards and committees will be subject to a duty analogous to that set out in reg 2.1 of the *Public Service Regulations*—that is, a duty not to disclose information that has come to a member’s knowledge or into a member’s possession by reason of being a member of the board or committee, where the disclosure is reasonably likely to be prejudicial to the effective working of government. The relevant exceptions to the obligation of non-disclosure—for example, for information that is already in the public domain—should also be imported. Where the most closely related Commonwealth employment situation for a board or committee involves different non-disclosure requirements from those set out in

---

132 See, eg, *Australian Heritage Council Act 2003* (Cth) s 13(a); *Fuel Quality Standards Regulations 2001* (Cth) reg 12(a); *Plant Breeder’s Rights Act 1994* (Cth) s 64(5).

133 Proposal 14–1.

reg 2.1,<sup>134</sup> those different obligations are also likely to be appropriate for the board or committee.

14.123 There may be some boards and committees that perform such a distinct role or have access to such particular information that no reasonable comparison can be made with the secrecy obligations that apply to Commonwealth employees. In these circumstances, the duty of non-disclosure should be at the discretion of the responsible minister or agency.

14.124 The ALRC further proposes that the terms and conditions of appointment of members of Commonwealth boards and committees should specify the right to terminate the member for breach—for example, through a broader misconduct provision or as a stand-alone ground for termination. This ensures that there is a mechanism to enforce the obligation of secrecy.

**Proposal 14–4** The Australian Government should include in the terms and conditions of appointment for members of boards and committees:

- (a) secrecy requirements equivalent to those imposed on Commonwealth employees in a related employment context, to the extent that these requirements are consistent with the board's or committee's function and structure; and
- (b) the right to terminate the appointment of a member in the event of a breach of the secrecy obligation.

### State and territory public sector employees

14.125 In IP 34, the ALRC asked in what circumstances Commonwealth secrecy provisions should apply to—among others—state and territory government employees.<sup>135</sup> Employees of state and territory governments may receive Commonwealth information, for example, in connection with an inter-jurisdictional program or committee.

14.126 Public sector employees in most Australian states and territories are subject to duties of non-disclosure either through legislation or whole of government codes of conduct. In NSW, for example, the *Model Code of Conduct for NSW Public Agencies*, issued by the Department of Premier and Cabinet, requires NSW Government agencies to have in place ‘clearly documented procedures regarding the storage, disclosure and distribution of confidential or sensitive personal, commercial or political

134 The situations where the obligation of non-disclosure that applies to a Commonwealth employee may differ from reg 2.1 are discussed above.

135 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–1.

information'.<sup>136</sup> Employees must handle such information in accordance with these procedures and 'must take special precautions to make sure that it is not disclosed without clear authority'.<sup>137</sup>

14.127 The Victorian public sector is governed by the *Code of Conduct for Victorian Public Sector Employees*.<sup>138</sup> This document has been issued by the Victorian Public Sector Standards Commissioner under the authority provided by s 63 of the *Public Administration Act 2004* (Vic). Under the Code, employees must

only disclose official information or documents acquired in the course of their public employment when required to do so by law, in the legitimate course of duty, when called to give evidence in court, or when proper authority has been given.<sup>139</sup>

14.128 South Australia has in place the most detailed codification of the circumstances when the disclosure of official information by public sector employees will be permissible. Under s 57 of the *Public Sector Management Act 1995* (SA), an employee is liable to disciplinary action if he or she discloses information gained in his or her official capacity, except as authorised under the regulations. That is, where disclosure:

- (a) is required as part of the employee's official duties; or
- (b) is required or authorised under the *Freedom of Information Act 1991* or the *Whistleblowers Protection Act 1993* or is otherwise required by law; or
- (c) is made with the permission of the Chief Executive of the administrative unit in which the employee is employed; or
- (d) —
  - (i) does not give rise to any reasonably foreseeable possibility of prejudice to the Government in the conduct of its policies, having regard to the nature of the disclosure or comment, the employee's current position or previous positions in the Public Service and the circumstances in which the disclosure or comment is made; and
  - (ii) is not made with a view to securing a pecuniary or other advantage for the employee or any other person; and
  - (iii) does not involve—
    - (A) any disclosure of information contrary to any law or lawful instruction or direction; or

---

136 New South Wales Premier's Department, *Model Code of Conduct for NSW Public Agencies* (1997), 6.

137 Ibid.

138 Victorian Government State Services Authority, *Code of Conduct for Victorian Public Sector Employees* (2007) <<http://www.ssa.vic.gov.au/>> at 6 March 2009.

139 Ibid, [3.4]. The *Public Sector Employment and Management Regulations 1998* (NT) sets out similar requirements for the disclosure of official information. Disclosure is permitted 'as required by law' or 'where proper authority has been given': [10.1].

- 
- (B) any disclosure of trade secrets or information of commercial value the disclosure of which would diminish its value or unfairly advantage a person in commercial dealings with the Government; or
  - (C) any disclosure of information in breach of intellectual property rights.<sup>140</sup>

14.129 In the ACT, a public servant is prohibited, without lawful authority, from disclosing ‘any information acquired by him or her as a consequence of his or her employment’ or ‘any information acquired by him or her from any document to which he or she has access as a consequence of his or her employment’.<sup>141</sup> The *State Service Act 2000* (Tas) requires Tasmanian public servants to maintain ‘appropriate confidentiality’ about information that they acquire in the course of employment.<sup>142</sup> Public sector obligations under the Western Australian legislation include an obligation not to use ‘for any purpose other than the discharge of official duties as an officer, information gained by or conveyed to that officer through employment in the Public Service’.<sup>143</sup>

14.130 The Queensland regime focuses on the procedure for developing public sector codes of conduct, as opposed to the substantive content of agency codes.<sup>144</sup> The ALRC anticipates, however, that the vast majority of public sector codes will include a duty of non-disclosure. For example, the *Code of Conduct for People Working in Queensland Transport* prevents an employee from using or disclosing any ‘sensitive’ or ‘confidential’ information that he or she gains by working for the department other than in limited circumstances.<sup>145</sup>

14.131 All Australian governments have agreed through a memorandum of understanding to comply with the minimum protective security standards contained in the PSM for handling national security information.<sup>146</sup>

### ***Submissions and consultations***

14.132 A small number of stakeholders expressed support for applying secrecy provisions to state and territory public sector employees. The Australian Transaction Reports and Analysis Centre (AUSTRAC) expressed the view that state and territory

---

140 *Public Sector Management Regulations 1995* (SA) reg 15.

141 *Public Sector Management Act 1994* (ACT) s 9.

142 *State Service Act 2000* (Tas) s 9.

143 *Public Service Regulations 1988* (WA) reg 8.

144 The *Public Sector Ethics Act 1994* (Qld) provides that a code ‘may contain anything the responsible authority considers necessary or useful for achieving the purpose of a code of conduct’: s 14.

145 Disclosure is permitted, eg, where an employee is lawfully allowed to disclose the information; the information is on the public record; the information was supplied for a purpose which allows disclosure; or where the consent of the individual has been obtained: Queensland Transport, *Code of Conduct for People Working in Queensland Transport* (2008), 17–18.

146 See New South Wales Department of Premier and Cabinet, *NSW Policy and Guidelines for Protecting National Security Information*, M2008–17 (2008).

government agencies that access AUSTRAC information should be subject to the same non-disclosure provisions as Australian Government agencies.<sup>147</sup>

14.133 The ATO noted, in relation to state and territory government employees, that any information disclosed to such a person remains ‘protected tax information’ and therefore protected under the tax secrecy provision under which it was disclosed. The ATO considered this was appropriate.<sup>148</sup>

#### *ALRC’s views*

14.134 The ALRC does not consider at this stage that there is a need to propose any reforms to the administrative framework for state and territory public sector employees who access Commonwealth information. These persons are subject to state and territory legislative and administrative secrecy requirements. In the particular context of national security information, the states and territories have agreed to comply with protective security measures set out in the PSM. Similar arrangements could be made to accommodate any other specific concerns about information-sharing with state and territory public sectors that arise in the future.<sup>149</sup>

#### **No relationship with the Commonwealth**

14.135 The discussion above has focused on people who are connected to the Commonwealth, either through employment or some other relationship. However, sometimes information will come into the hands of people who do not have any relationship with the Commonwealth. For example, the case of *R v Goreng Goreng* concerned the disclosure of certain information by Ms Tjanara Goreng Goreng to her daughter and to a member of the administration of an Indigenous community.<sup>150</sup> Although both criminal and administrative disciplinary penalties were available in relationship to the conduct of Goreng Goreng herself, no administrative (or other non-criminal) penalties would have been available to address any further disclosure by her daughter or the community member.

14.136 The Australian Press Council noted the difficulties that the lack of disciplinary penalties can create for private sector employees, such as the media:

Whereas the conduct of government employees is regulated by legislation and internal administrative procedures, which specify the officer’s duties and obligations with regard to information handling, a journalist or editor is subject only to criminal legislation ... This raises difficulties, which need to be considered when framing

---

147 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

148 Australian Taxation Office, *Submission SR 13*, 16 February 2009. See also Department of Climate Change, *Submission SR 27*, 23 February 2009.

149 For example, such arrangements could be considered as part of a framework for sharing inter-jurisdictional criminal history information about people who work with children. The need for information sharing in this context was affirmed by the Council of Australian Governments on 29 November 2008: Council of Australian Governments (COAG), *Council of Australian Governments’ Meeting Communiqué*, 29 November 2008.

150 *R v Goreng Goreng* [2008] ACTSC 74. This case is discussed in Ch 2.

secrecy legislation. Because media professionals are not subject to the disciplinary processes, which are available in relation to public servants, a situation may arise where a minor disclosure that is ostensibly in the public interest is treated as a breach of secrecy warranting criminal conviction. By contrast, a public servant making a disclosure of the same information for the same purpose might instead be disciplined by way of a range of internal mechanisms, even though the duty breached is arguably a higher one than that breached by the journalist.<sup>151</sup>

14.137 In Chapter 6, the ALRC discusses the three civil penalty secrecy provisions currently on the Commonwealth statute book. The ALRC suggests that two of these potentially could be recast as criminal provisions or contractual requirements. Section 276 of sch 1 of the *Workplace Relations Act 1996* (Cth), however, does not fall neatly into either of these constructions. This raises the question whether gaps remain in the ALRC's proposed framework for regulating the disclosure of Commonwealth information and, if so, whether there is a role for civil penalty provisions in addressing this gap. In particular, the ALRC is interested in stakeholders' views on the appropriateness of applying civil penalty provisions to private sector persons who have access to Commonwealth information other than in a contractual setting.

14.138 As discussed elsewhere in this Discussion Paper, the equitable duty of confidence results from the nature of information and the circumstances of its disclosure: it is not contingent on a particular relationship between the parties. Enforcement of these duties via the action for breach of confidence or damages for breach of contract may provide an adequate alternative to criminal proceedings for persons that are not otherwise in a relationship with the Commonwealth.

**Question 14–1** Are there any situations in which neither administrative penalties nor contractual remedies apply to an unauthorised disclosure of Commonwealth information? If so, are civil penalties a suitable way to address these gaps in application or are there other, better ways of dealing with these situations?

## Lawful and reasonable employer directions

14.139 The employment obligations of Commonwealth employees are not limited to requirements directly set out in the *Public Service Act* or other express terms and conditions in the employment contract. Obligations under another law, for example, a criminal secrecy offence, could be implied as a necessary incident of an employment contract if, without it, the contract would be 'seriously undermined'.<sup>152</sup> Moreover, as

151 Australian Press Council, *Submission SR 16*, 18 February 2009.

152 *Liverpool CC v Irwin* [1977] AC 239, approved and followed in *Byrne v Australian Airlines Limited* (1995) 185 CLR 410. The APS Code of Conduct requires that APS employees must comply with all applicable Australian laws when acting in the course of APS employment: *Public Service Act 1999* (Cth) s 13(4).

set out below, all employees, including Commonwealth employees, must comply with any ‘lawful and reasonable direction’ issued by their employer.

14.140 The scope of the common law duty to comply with lawful and reasonable directions is discussed in detail in Chapter 13. In particular, employees are obliged to comply with a command that ‘relates to the subject matter of the employment’, ‘involves no illegality’ and is ‘reasonable’.<sup>153</sup> In the context of the public service, a somewhat broader test for the lawfulness of directions is likely to apply.<sup>154</sup>

14.141 Employer directions have the potential to override many of the administrative reforms suggested in this Discussion Paper. Whistleblowers Australia advised in its submission on IP 34, for example, that the Chief Executive Officer of the Australian Customs Service had previously issued a direction that ‘any and all information obtained by or generated in the Customs service’ was protected information and subject to a duty of non-disclosure. Whistleblowers Australia commented that ‘some boundaries’ must be placed on what secrecy directions can be given by an agency head.<sup>155</sup>

14.142 In *Bennett v President, Human Rights and Equal Opportunity Commission*,<sup>156</sup> Finn J held that a direction issued by an Australian Government agency to employees will not be ‘lawful and reasonable’ where it infringes the implied constitutional guarantee of freedom of communication about government and political matters.<sup>157</sup> As expressed by Finn J:

It is not sufficient simply to contend that [an agency] gave lawful and reasonable directions with which [the employee] was bound to comply when there would be a real issue between the parties as to whether the directions given were lawful and reasonable.<sup>158</sup>

### **ALRC’s views**

14.143 A focus of the ALRC’s proposals in this and the preceding chapter is on establishing a consistent and effective administrative secrecy framework in the Australian Government. In particular, the ALRC is of the view that the conduct requirements in reg 2.1 of the *Public Service Regulations*, as revised in Proposals 13–1 to 13–3, should be the standard administrative secrecy obligation that applies to Commonwealth employees. In Chapter 15, the ALRC proposes that Australian Government agencies should develop and implement information-handling policies

---

153 *R v Darling Island Stevedoring & Lighterage Co Ltd; Ex parte Halliday* (1938) 60 CLR 601, 621–622.

154 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor. The AGS has advised that a direction to an APS employee can be lawful if it involves no illegality; is reasonably adapted to protect the legitimate interests of the Commonwealth; and is reasonable in all the circumstances: *ibid*.

155 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

156 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

157 The implied constitutional freedom of political communication is discussed extensively in Ch 2.

158 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [121].

that clarify the application of this obligation in the particular context of their information holdings.<sup>159</sup> This combination provides a sufficiently nuanced secrecy framework to avoid the need for agencies to issue further directions to their employees on the non-disclosure of information.

14.144 There may be some limited situations where the potential consequences of the disclosure of Commonwealth information, or another circumstance, justify an agency giving directions to its employees over and above the requirements set out in reg 2.1. For example, an agency that very rarely deals with national security information may need to access classified material for the purposes of a particular project. The agency could issue a direction to its employees imposing specific information-handling rules for the classified material. In this context, the principal limitation to an agency's discretion is the relationship between the direction and the implied constitutional freedom of political communication.

14.145 The ALRC proposes that Australian Government agencies that have in place administrative secrecy requirements which differ from the revised reg 2.1, including 'lawful and reasonable directions' issued to employees, should review these requirements for consistency with the implied constitutional freedom of political communication.

**Proposal 14–5** Australian Government agencies should review administrative secrecy requirements that differ from the revised reg 2.1 of the *Public Service Regulations 1999* (Cth), including 'lawful and reasonable directions' issued to employees to ensure that these are consistent with the implied constitutional freedom of political communication.

159 Proposal 15–1.



# **15. Fostering Effective Information-Handling Practices**

---

## **Contents**

Introduction	523
An effective information-handling culture	524
Risk factors for inappropriate information handling	525
Agency policies and guidelines	526
Submissions and consultations	528
ALRC's views	530
Memorandums of understanding	533
Submissions and consultations	534
ALRC's views	535
Training and development programs	536
Submissions and consultations	537
ALRC's views	538
Oaths, affirmations and acknowledgements of secrecy	539
Submissions and consultations	541
ALRC's views	541
Information and communication technology systems	542
Submissions and consultations	543
ALRC's views	544
Avenues for employee queries and concerns	544
ALRC's views	545
Fostering effective information handling at the agency level	546
Commonwealth Ombudsman	546
Australian Public Service and Merit Protection Commissioners	547
Australian National Audit Office	548
Information Commissioner	549
Overseeing specific sectors	549
Submissions and consultations	552
ALRC's view	553
Fostering effective information handling in the private sector	554

## **Introduction**

15.1 Previous chapters of this Discussion Paper have focused on the legal obligations of non-disclosure that should attach to Commonwealth officers and others who handle Commonwealth information. Secrecy laws, however, do not operate in a vacuum.

Other laws and practices will influence whether or not an entity publishes or an individual discloses Commonwealth information, including freedom of information (FOI) and privacy laws, and the broader information-handling culture within which the individual is situated.

15.2 Australian Government agencies employ a range of strategies to guide the release of Commonwealth information by individual officers, including:

- developing and implementing written policies, manuals and guidelines governing when Commonwealth information should be shared and when it should be kept secret, such as the *Australian Government Protective Security Manual* (PSM), agency policies on information handling, and memorandums of understanding (MOUs);
- raising individual officers' awareness of their information-handling obligations through leadership and development programs and oaths of secrecy; and
- implementing infrastructure suitable for handling and securing particular types of Commonwealth information; in particular, information and communication technology (ICT) systems.

15.3 Australian Government agencies also have frameworks in place governing the disclosure of information in accordance with the *Freedom of Information Act 1982* (Cth) (FOI Act) and as a matter of general policy and practice. The relationship between secrecy and the FOI Act is discussed in detail in Chapter 4.

15.4 This chapter discusses the extent to which the above strategies contribute to the compliance of Commonwealth officers with secrecy laws and other information-handling obligations, and makes suggestions for possible improvements. The chapter goes on to consider information handling at the level of Australian Government agencies, and in particular the role of independent oversight bodies in fostering an effective information-handling culture at the agency level. Finally, the chapter considers the handling of Commonwealth information in the private sector.

## An effective information-handling culture

15.5 The overarching premise of this chapter is the need for Australian Government agencies and others to foster an effective information-handling culture, rather than what has been described as a 'culture of secrecy'.

15.6 As has been commented on extensively in the context of freedom of information, there are compelling drivers for agencies and officers to sacrifice the goals of openness and accountability because of a real or perceived need for non-disclosure. The 'culture of secrecy' was criticised by the ALRC and the Administrative Review Council in the 1995 report, *Open Government: A Review of the Federal*

*Freedom of Information Act 1982* (ALRC 77).<sup>1</sup> In 2008, the Independent Review Panel examining the *Freedom of Information Act 1992* (Qld) discussed the tension inherent in information management:

Inherent at an organisational level, the urgency of the everyday imperatives in modern government can pull the public sector's information culture towards information protection in the interests of issues management, at the expense of the important but less urgent information goals for transparency in government. ...

Culture brings a more complex setting. Access to government information reaches to the core of political and bureaucratic interests and operates beyond purely legal considerations and dispassionate calculations on the public interest.<sup>2</sup>

15.7 In its submission to the Issues Paper, *Review of Secrecy Laws* (IP 34),<sup>3</sup> the Australian Government Attorney-General's Department (AGD) noted that a number of reviews have considered the impact of secrecy laws on information sharing and indicated that cultures of secrecy within some of the relevant agencies pose a greater barrier to information sharing than legislative restrictions.<sup>4</sup>

15.8 An effective information-handling culture minimises unauthorised handling of Commonwealth information, while encouraging information sharing in appropriate circumstances—or, to put this in another way, it produces an administrative regime that institutes a suitable balance between the ‘need to know’ and the ‘need to share’ principles.

### Risk factors for inappropriate information handling

15.9 The Queensland Crime and Misconduct Commission (QCMC) has identified a number of risk factors that are associated with the unauthorised disclosure of official information, including intentional non-compliance—that is, the deliberate ‘leaking’ or inappropriate withholding of Commonwealth information—and unintentional non-compliance.

15.10 The QCMC notes that, among other factors, the *deliberate* release of information may be motivated by:

- personal motivations, such as the sale of information for profit or personal advantage, or dissatisfaction with the stifling of debate, or the ignoring of the officer’s individual or professional views;

---

1 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Ch 4.

2 Freedom of Information Review Panel, *Enhancing Open and Accountable Government*, Discussion Paper (2008), 90–91.

3 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

4 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

- disgruntlement because of, for example, a failure to gain promotion, dismissal or other disciplinary action; and
- an inappropriate organisational culture such as a failure to consistently condemn the misuse or unauthorised release of information or a practice of misuse or unauthorised release by senior management.<sup>5</sup>

15.11 Risk factors for the *unintentional* release of information include:

- inadequate or unclearly articulated policies and procedures on information management;
- procedural issues, such as a failure to classify sensitive information properly or poor recordkeeping practices; and
- failings in network and computer security, such as inadequate guidelines on password use and computer security, the unauthorised removal of electronic material from the office or malicious network breach.<sup>6</sup>

15.12 Similar issues may contribute to a failure to share information in appropriate circumstances. For example, personal motivations may result in a Commonwealth officer deliberately withholding information where disclosure could reveal malfeasance. Information-handling policies that do not clearly identify the circumstances in which information can be disclosed to Australian Government agencies or others may result in an officer not revealing information that could properly be shared—or a lengthy delay before such sharing occurs.

15.13 In the following sections of this chapter, the ALRC considers strategies that can be put in place by Australian Government agencies and others to encourage compliance with secrecy laws on the one hand, and information-handling objectives—such as privacy and FOI—on the other.

## **Agency policies and guidelines**

15.14 The guide issued for Australian Public Service (APS) employees by the Australian Public Service Commission (APSC), *APS Values and Code of Conduct in Practice*, advises that:

---

<sup>5</sup> Crime and Misconduct Commission Queensland, *Information Security—Keeping Sensitive Information Confidential*, Building Capacity Series Number 7 (2005), 4. Suggestions about an agency culture of inappropriately releasing information were raised, for example, in P Durbin, ‘ATO lashed over privacy breaches’, *Australian Financial Review*, 23 April 2009, 1.

<sup>6</sup> Crime and Misconduct Commission Queensland, *Information Security—Keeping Sensitive Information Confidential*, Building Capacity Series Number 7 (2005), 5.

Agencies should establish clear policies and guidelines so that employees are aware of the provisions that govern the management of information. In addition, agencies may care to consider issuing directions:

- that require APS employees to comply with agency-level protective security policies and instructions developed on the basis of the PSM;
- to specific groups of APS employees working with particular kinds of information (for example, APS employees working on a particular tender exercise);
- that require APS employees to seek advice if they are unsure about whether to disclose information and to keep a record of that advice if authorised to disclose information.<sup>7</sup>

15.15 Agency policies and guidelines can foster compliance with secrecy laws and other information-handling obligations by instilling confidence in agency employees and others about the types of information that can be disclosed and the processes for disclosure.<sup>8</sup> For example, the *Protocol Governing the Disclosure of Information Between the Child Support Agency and Centrelink* specifically identifies the information that can lawfully be shared between Centrelink and the Child Support Agency (CSA).<sup>9</sup> Where an agency requests information other than the data items that have been expressly authorised under the protocol, it must specify why the information is needed and the legislative basis for the disclosure.<sup>10</sup>

15.16 In some situations, an Australian Government agency may issue a policy to deal with a specific contentious or problematic secrecy issue. This is illustrated, for example, by the Australian Taxation Office (ATO) practice statement, *Disclosure to Ministers of Information about the Affairs of Taxpayers*, which clarifies the circumstances in which ATO officers can provide information about a taxpayer to a minister, including for the purpose of responding to ministerial correspondence with the individual about whom the information relates.<sup>11</sup>

7 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 23 September 2008, Ch 3.

8 See, eg, comments about the need to clarify information sharing between the Australian Federal Police and the Australian Security Intelligence Organisation in Australian Federal Police National Security Operations Review Committee, *The Street Review: A Review of Interoperability Between the AFP and its National Security Partners* (2008), [4.2].

9 Australian Government Child Support Agency and Centrelink, *Protocol Governing the Disclosure of Information Between the Child Support Agency and Centrelink 1 October 2006–30 September 2008*. Information that Centrelink can disclose to the CSA under child support legislation includes, among other details, customer name, the last known customer address, family tax benefit entitlements for customers with outstanding debts, last known employment details and last known bank account details: attachment A. In return, the CSA can disclose to Centrelink, upon request, details of applications for child support, any current or previous entitlements of Centrelink customers to child support, and details of disbursed payments: attachment B.

10 Ibid, 3.

11 Australian Taxation Office, *ATO Practice Statement Law Administration: Disclosure to Ministers about the Affairs of Taxpayers*, PS LA 2004/9 (2004).

15.17 Agency policies can also promote awareness among employees of the avenues through which an employee can raise queries and concerns about their secrecy and other information-handling obligations.<sup>12</sup>

15.18 Tensions can arise, however, where an agency policy imposes more restrictive information-handling obligations than required by law. This issue came into focus, for example, in hearings before the Senate Select Committee on a Certain Maritime Incident (the Children Overboard affair). The Committee heard evidence about the Department of Defence's public affairs policy, which essentially required all information to be released only by the Minister's media adviser. In its final report on the incident, the Senate Select Committee noted that:

the strictly centralised control of information through the Minister's office ... meant that Defence was unable to put out even factual information without transgressing the public affairs plan.<sup>13</sup>

### **Submissions and consultations**

15.19 In IP 34, the ALRC asked whether agencies' policies on information handling were consistent with Commonwealth secrecy laws. In particular, the ALRC sought views on whether agency policies were imposing more restrictive information-handling practices than those required under the related secrecy provisions.<sup>14</sup>

15.20 Several Australian Government agencies advised that their information-handling policies were consistent with relevant secrecy provisions.<sup>15</sup> Other agencies justified the need for departure from the legislative standards in some circumstances. For example, the Australian Securities and Investments Commission (ASIC) advised that, in the management of high profile investigative or regulatory matters, it sometimes applies more stringent secrecy controls than those set out in Commonwealth secrecy laws and other relevant standards and guidelines.<sup>16</sup>

15.21 The AGD commented that agency policies on information handling are not solely directed towards an objective of secrecy:

Where agency policies are broader than secrecy laws, this may reflect the different objectives behind these policies. For example, agencies may have a policy that all media enquiries are to be referred to the public affairs area or to the Minister's Office.

---

12 See, eg, Australian Taxation Office, *ATO Practice Statement: Secrecy and Privacy Obligations*, PS CM 2004/07 (2004), which directs employees who are in doubt about whether an action is lawful under the *Privacy Act* or secrecy laws to seek advice from their manager, the relevant Privacy Network member, and, if necessary, the Legal Services Branch: 3.

13 Parliament of Australia—Senate Select Committee on a Certain Maritime Incident, *Majority Report* (2002), [2.53].

14 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–1.

15 Australian Intelligence Community, *Submission SR 37*, 6 March 2009; Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

16 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

Such policies may be directed towards ensuring the dissemination of accurate information and also at upholding the value of an apolitical public service.<sup>17</sup>

15.22 On the other hand, the Public Interest Advocacy Centre (PIAC) expressed the view that, if agency policies purported to impose higher levels of secrecy than those that arise under Commonwealth secrecy laws, the agency should have to make out a ‘convincing case’ to justify them.<sup>18</sup> Liberty Victoria noted the ‘impossible position’ that Commonwealth officers can be placed in when there is conflict between agency policies and guidelines, and legislative secrecy requirements.<sup>19</sup>

15.23 The Community and Public Sector Union (CPSU) commented on the need to clearly identify the source and effect of secrecy obligations. The CPSU recommended that Commonwealth information should be clearly divided into secret information that is subject to criminal sanctions; Commonwealth information that may be subject to other non-disclosure or confidentiality duties; and other Commonwealth information. It expressed the view that guidance materials on these employment-based duties should be provided to APS employees and APS management.<sup>20</sup>

15.24 The Australian Press Council and PIAC both submitted that individual agency information-handling policies should be publicly released.<sup>21</sup> The Press Council noted that this would facilitate actions for judicial review and ‘enable citizens to develop an understanding of the extent and character of secrecy processes’.<sup>22</sup> It further submitted that:

any regulatory mechanisms that define the duty of officers to keep information confidential should be contained in legislation that is subject to parliamentary scrutiny, not in subordinate legislation ... It is not appropriate that governments can extend or alter the level of secrecy, which officers are obligated to administer, without having to justify the change to the elected representatives of the Australian people.<sup>23</sup>

15.25 PIAC also commented on the need to clarify the relationship between agency information-handling policies and the ‘lawful and reasonable direction’ requirement under s 13(5) of the *Public Service Act 1999* (Cth).<sup>24</sup>

17 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

18 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

19 Liberty Victoria, *Submission SR 19*, 18 February 2009.

20 Community and Public Sector Union, *Submission SR 32*, 2 March 2009. The NSW Young Lawyers Human Rights noted the need to identify in guidelines the relevant legislation relating to the duty not to disclose government information: NSW Young Lawyers Human Rights Committee, *Submission SR 34*, 4 March 2009.

21 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009; Australian Press Council, *Submission SR 16*, 18 February 2009.

22 Australian Press Council, *Submission SR 16*, 18 February 2009.

23 Ibid.

24 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009. Lawful and reasonable directions are discussed in Ch 14.

### **ALRC's views**

15.26 The primary objective of agency information-handling policies is to clarify for Commonwealth officers and others who handle Commonwealth information the application of secrecy laws and other information-handling obligations. Agency policies can also satisfy a secondary role of assisting members of the public in understanding the standard of openness that they should expect from government.

15.27 As discussed in detail below, recognising the role of agency policies as one of clarifying the application of information-handling obligations goes a long way towards addressing the possible tension where agency policies require a different level of secrecy to that imposed under related Commonwealth secrecy provisions.

15.28 The ALRC is proposing two further reforms in the context of agency information-handling policies. First, the establishment of baseline requirements for information that Australian Government agencies must include in their information-handling policies—in particular, the classes of information that can be disclosed to others and any associated penalties for unauthorised disclosure.<sup>25</sup> Secondly, Australian Government agencies should make their information-handling policies publicly available.<sup>26</sup> These proposals are discussed further below.

#### ***Level of secrecy in information-handling policies***

15.29 Commonwealth officers and others who handle Commonwealth information can be placed in a difficult situation when they are subject to an agency information-handling policy that imposes a different level of secrecy from requirements under legislation and the general law. For example, an agency policy could restrict all but a select few officers from releasing information to ministerial staffers, including publicly available information. This is more stringent than the proposed general secrecy offence<sup>27</sup> and the administrative secrecy obligations presently set out in reg 2.1 of the *Public Service Regulations 1999* (Cth).<sup>28</sup> These both include exceptions for information in the public domain. Moreover, an officer may be of the view that compliance with this information-handling policy conflicts with other requirements of his or her employment—for example, his or her duty to provide the government with ‘frank, honest, comprehensive, accurate and timely advice’.<sup>29</sup>

15.30 If agency information-handling policies are drafted correctly, this normally will mean that the level of secrecy imposed under the policy will be equivalent to that set out in related Commonwealth secrecy laws or employee directions. However, in certain circumstances, other legal requirements may justify an agency imposing a

---

25 Proposal 15–1.

26 Proposal 15–2.

27 The exceptions to the proposed general secrecy offence are discussed in Ch 9.

28 Administrative secrecy obligations are discussed in Chs 13 and 14. *Public Service Regulations 1999* (Cth) reg 2.1 applies to APS employees. The ALRC is proposing that this obligation should be the default administrative secrecy obligation for all Commonwealth employees: Proposal 13–1.

29 *Public Service Act 1999* (Cth) s 10(1)(f).

different level of secrecy. In the scenario set out in the preceding paragraph, for example, the agency may have decided that restricting the employees who can provide information to ministerial staff was necessary to ensure that the advice it provided to the government was ‘apolitical’ and ‘accurate’.<sup>30</sup> In order for the policy to be properly characterised as ‘clarifying’ the information-handling obligations of officers—rather than imposing new and different secrecy requirements—the agency should clearly set out the objectives upon which it relies to justify the discrepancy.

#### ***Baseline requirements for information-handling policies***

15.31 The ALRC proposes that agency information-handling policies should include a baseline amount of information about the secrecy obligations that apply to officers, in addition to the potential consequences of breach.<sup>31</sup> Information-handling policies should clearly set out:

- the types of information that an employee can routinely disclose in the performance of his or her duties;
- the types of information for which an employee should obtain authority for disclosure, including the potential for unauthorised disclosure to result in administrative disciplinary action; and
- situations where the unauthorised handling of information could result in criminal proceedings.

15.32 In Chapter 13, the ALRC proposes that agency information-handling policies should also clarify the manner in which an agency will apply administrative penalties for breaches of secrecy provisions.<sup>32</sup>

15.33 Including these types of information in agency policies may foster effective information-handling practices by Commonwealth officers and others in a number of ways. First, it gives an unambiguous statement of situations when disclosing Commonwealth information will be unlawful, thereby minimising unintended breaches. Secondly, information about the potential consequences of unauthorised disclosure of Commonwealth information can reinforce the deterrent effect of criminal and administrative secrecy penalties, thereby lessening intentional breaches. Finally, instilling a greater confidence in Commonwealth officers about situations where disclosing information is lawful can promote the timely sharing of Commonwealth information in appropriate circumstances.

---

<sup>30</sup> Ibid.

<sup>31</sup> Proposal 15–1.

<sup>32</sup> Proposal 13–5.

15.34 The ALRC also proposes that agency information-handling policies should include information on the avenues available to Commonwealth officers to raise queries or concerns. This is discussed later in this chapter.

### ***Making policies publicly available***

15.35 The ALRC proposes that Australian Government agencies should publish their information-handling policies.<sup>33</sup> The public release of government policies provides members of the public with a better understanding of the standard of openness that they should expect from Australian Government agencies. A greater degree of transparency in the day-to-day operation of secrecy laws also keeps the Australian Government accountable to the public on its information-sharing processes.

15.36 Making Australian Government information-handling policies publicly available is consistent with the object of the FOI Act of

making available to the public information about the operations of departments and public authorities and, in particular, ensuring that rules and practices affecting members of the public in their dealings with departments and public authorities are readily available to persons affected by those rules and practices.<sup>34</sup>

15.37 The need for public availability of government information is stressed even more strongly in the revised objects clause included in the Exposure Draft of the Freedom of Information Amendment (Reform) Bill 2009 (Cth).

- (1) The objects of this Act are to give the Australian community access to information held by the Government of the Commonwealth, by:
  - (a) requiring agencies to publish the information; and
  - (b) providing for a right of access to documents.
- (2) The Parliament intends, by these objects, to promote Australia's representative democracy by contributing towards the following:
  - (a) increasing public participation in Government processes, with a view to promoting better-informed decision-making;
  - (b) increasing scrutiny, discussion, comment and review of the Government's activities.<sup>35</sup>

15.38 In the ALRC's view, the vast majority of Australian Government information-handling policies should be publicly available. This includes, for example, many parts of the PSM, as recommended by the ALRC in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98).<sup>36</sup> However, there may be

<sup>33</sup> Proposal 15–2.

<sup>34</sup> *Freedom of Information Act 1982* (Cth) s 3(1)(a).

<sup>35</sup> Freedom of Information Amendment (Reform) Bill 2009 (Cth)—Exposure Draft, sch 1 s 3.

<sup>36</sup> Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 4–1. At the time of ALRC 98, the PSM did not have a security classification but was not publicly available. Since this time, the document has been given a security classification. The PSM and security classifications are discussed in Ch 3.

exceptional cases where it would not be reasonable to publish information on the disclosure protocols of Australian Government agencies. For example, it may be that public knowledge of the information holdings of an intelligence agency, or its patterns of information sharing, could impede the agency's functions. The ALRC proposes that there should be an exception from the general requirement of public release of information-handling protocols where such release would be 'unreasonable or impractical'.

**Proposal 15–1** Australian Government agencies should develop and implement policies clarifying the application of relevant secrecy laws to their information holdings. These policies should include:

- (a) the types of information that an employee can lawfully disclose in the performance of his or her duties;
- (b) the types of information for which an employee must obtain authority for disclosure, including the potential for unauthorised disclosure to result in disciplinary action;
- (c) the circumstances in which the unauthorised handling of information could lead to criminal proceedings; and
- (d) avenues for an employee to raise queries or concerns, including the process by which he or she can make a public interest disclosure.

**Proposal 15–2** Australian Government agencies should make their information-handling policies publicly available, save in certain exceptional cases where this would be unreasonable or impractical.

## Memorandums of understanding

15.39 Australian Government agencies that regularly share information with other agencies or bodies can formalise the terms of exchange through an MOU. This may provide an additional tool to facilitate compliance with information-handling obligations.<sup>37</sup>

15.40 An MOU does not of itself provide a legal basis for the handling of Commonwealth information. Its operation must be underpinned by common law or statute. However, entry into an MOU may promote appropriate information sharing among agencies and others. While acknowledging that MOUs generally do not have the force of law, the Administrative Review Council has advised that they may regulate

37 Chapter 3 discusses MOUs in the context of sharing Commonwealth information.

the exchange of information among government agencies by ‘formalis[ing] the terms of a relationship or framework for cooperation between the parties’.<sup>38</sup>

15.41 Several Australian Government agencies have MOUs in place relevant to information handling. For example, ASIC has entered into an MOU with the Australian Government Financial Reporting Council, under which the entities agree—subject to any restrictions imposed by law—to ‘share information that they believe would be of assistance to the other in understanding their respective responsibilities under the law’.<sup>39</sup> Each agency agrees, on request, to provide certain information to the other in a timely manner.<sup>40</sup> They further agree to use ‘reasonable endeavours’ to notify the other of the existence of relevant information, notwithstanding that the information has not been requested.<sup>41</sup> Commonwealth and state and territory police departments also have entered into a detailed MOU for the sharing of law enforcement information.<sup>42</sup>

### **Submissions and consultations**

15.42 In IP 34, the ALRC asked about the effectiveness of the strategies used by Australian Government agencies—such as MOUs—in protecting Commonwealth information.<sup>43</sup>

15.43 The AGD noted that ‘MOUs and similar instruments may be used to set out a shared understanding and guidelines for the communication, handling and protection of particular information’.<sup>44</sup> The ATO agreed that MOUs were ‘an effective tool for setting up protocols for the exchange of information with other agencies’.<sup>45</sup> The Commonwealth Ombudsman also advised that it has entered into MOUs with some other agencies about the exchange of information, and that these appeared to be working well.<sup>46</sup>

15.44 Although the Australian Bureau of Statistics (ABS) agreed that MOUs can help to clarify information-handling obligations, it commented that, because MOUs between Commonwealth agencies are not legally enforceable, they are not guarantees

---

38       Administrative Review Council, *The Coercive Information-Gathering Powers of Government Agencies*, Report No 48 (2008), 65.

39       Australian Government Financial Reporting Council, *Memorandum of Understanding Between the Australian Securities and Investments Commission and the Financial Reporting Council* (2004) <[www.frc.gov.au/auditor/mou/MOU\\_ASIC.asp](http://www.frc.gov.au/auditor/mou/MOU_ASIC.asp)> at 28 May 2009 cl 4.1.

40       Ibid, cl 4.2.

41       Ibid, cl 4.3.

42       New South Wales Police and others, *Memorandum of Understanding between New South Wales Police, Victoria Police, Queensland Police, Western Australia Police, South Australia Police, Northern Territory Police, Tasmania Police, ACT Policing, Australian Federal Police and the CrimTrac Agency*.

43       Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–3(a).

44       Attorney-General’s Department, *Submission SR 36*, 6 March 2009. See also Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

45       Australian Taxation Office, *Submission SR 13*, 16 February 2009.

46       Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009. AUSTRAC also submitted that it has entered into MOUs with agencies that set out the measures that parties will put in place to protect the confidentiality of information: Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

of protection.<sup>47</sup> However, the AGD noted that, although MOUs are voluntary arrangements, they operate within the legal framework that governs the relevant parties to the agreement. In some cases, this framework may give legal force to certain agreements and obligations set out in the MOU.<sup>48</sup>

15.45 Although not specifically directed to the context of MOUs, the Commonwealth Ombudsman raised the potential for difficulties to arise when an employee of the Ombudsman needs to access another agency's documents that have a security classification. Although there is nothing in the *Ombudsman Act 1976* (Cth), or other legislation, to prevent access in these circumstances, Australian Government agencies are sometimes reluctant to provide the information other than in accordance with their own internal security classification procedures. While a course of action can usually be agreed upon, the issue can hamper speedy investigation.<sup>49</sup>

### ALRC's views

15.46 Almost all stakeholders that commented on this issue agreed that MOUs can be an effective tool for establishing the terms of exchange of information between an Australian Government agency and other agencies or bodies. In particular, MOUs formalise the standard information-sharing protocols between agencies. This minimises the need for ad hoc decision making on the part of individual Commonwealth officers and, consequently, the potential for inadvertent unauthorised disclosures. As with agency information-handling policies, an MOU may instil confidence in Commonwealth officers seeking to exchange information by creating certainty in the information-sharing framework. Where a disclosure is authorised under an MOU, it may also satisfy exceptions in criminal and administrative secrecy provisions for disclosures in the course of an employee's functions or duties. The ALRC proposes that Australian Government agencies that regularly share information with other agencies or bodies should enter into MOUs setting out the terms and conditions for the exchange of information.

15.47 A situation where an MOU may be useful, for example, is for the exchange of security classified information with a body such as the Commonwealth Ombudsman. Hypothetically, an MOU could be entered into between one or more Australian Government agencies and the Commonwealth Ombudsman, with the agency agreeing to share security classified information in defined circumstances. This could require, for example, the Ombudsman to abide by minimum protective security standards. Once an agreed framework was in place, investigations involving the use of classified information may be better able to proceed in a timely fashion.

---

47 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

48 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

49 Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009. This issue is also noted in Ch 3.

**Proposal 15–3** Australian Government agencies that regularly share information with other agencies or bodies should enter into memorandums of understanding setting out the terms and conditions for the exchange of information.

## Training and development programs

15.48 Training and development programs provide an opportunity for agencies to educate employees about their obligations in handling Commonwealth information, and to impart broader information-handling values.<sup>50</sup> In its *State of the Service Report 2001–02*, the APSC reported that agencies alerted employees to their obligations in relation to the non-disclosure of Commonwealth information through:

- the induction process (85% of agencies);
- promulgated policies (58% of agencies);
- Chief Executive instructions (46% of agencies); and
- training programs (44% of agencies).<sup>51</sup>

15.49 The APSC noted that although the majority of employees are informed of their obligations about Commonwealth information when they commence employment, 42% of agencies did not provide employees with regular reminders of these obligations.<sup>52</sup>

15.50 Some agencies have developed extensive training and development programs to advise employees and others about their information-handling responsibilities. Centrelink, for example, provides all graduates and cadets, on induction, with training on confidentiality, privacy and FOI laws. The training module, among other things, specifies the types of documents that officers can release outside the formal operation of the FOI Act; provides information on the application of privacy and secrecy laws;<sup>53</sup> and advises on the availability of contact officers to approach for further information.

<sup>50</sup> Sometimes training and development can also be used as an administrative action to address breaches of secrecy laws.

<sup>51</sup> Australian Public Service Commission, *State of the Service Report 2001–02* (2002), 28–29. More recent *State of the Service Reports* also include information about training and development activities; however, these do not specifically relate to the unauthorised disclosure of information.

<sup>52</sup> Ibid.

<sup>53</sup> Centrelink, *Centrelink Graduate and Cadet Induction: Confidentiality, Privacy, Freedom of Information* (2009).

## Submissions and consultations

15.51 In IP 34, the ALRC asked about the effectiveness of training and development programs in protecting Commonwealth information.<sup>54</sup>

15.52 Several Australian Government agencies advised that they placed a high degree of importance on training and development programs as a tool for protecting Commonwealth information.<sup>55</sup> The ABS, for example, advised that training was ‘a very effective strategy to maintain an organisational focus on secrecy and confidentiality’.<sup>56</sup> The ATO noted that all new staff members were required to undertake an extensive education and awareness program, including security, fraud and privacy training.<sup>57</sup> In addition to training programs on recruitment, the Australian Federal Police (AFP) advised that training on secrecy provisions forms a part of all management, leadership and supervisory developmental programs.<sup>58</sup>

15.53 One Australian Government agency noted that, in the past year, it had developed ‘a compulsory on-line training module’ and ‘policy instruction (with flow-charts and examples)’ to assist its officers to comply with secrecy laws. The agency provides in-person training to all entry-level officers, as well as training programs delivered on an ad hoc basis.<sup>59</sup>

15.54 The Australian Transaction Reports and Analysis Centre (AUSTRAC) noted that it also provides training and information to designated agencies and reporting entities on their record-keeping obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).<sup>60</sup>

15.55 In February 2009, the ALRC conducted an open forum about secrecy laws with members of the CPSU. Participants commented on the need for training and development programs to reflect the type of risks that are commonly encountered by employees of particular agencies. One participant noted that, unless the purpose of the provision is made relevant, employees go ‘straight to a fear culture’.<sup>61</sup> Callers to the ALRC’s secrecy phone-in also raised issues about the content of training and development programs. Callers made remarks about the need for Commonwealth

54 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–3(b).

55 Liberty Victoria also submitted that it supported the ‘thorough and ongoing training’ of all Commonwealth officers in the responsible handling of government information: Liberty Victoria, *Submission SR 19*, 18 February 2009.

56 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

57 Australian Taxation Office, *Submission SR 13*, 16 February 2009. See also Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009; Australian Intelligence Community, *Submission SR 37*, 6 March 2009; Attorney-General’s Department, *Submission SR 36*, 6 March 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009; Department of Human Services, *Submission SR 26*, 20 February 2009; Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

58 Australian Federal Police, *Submission SR 33*, 3 March 2009.

59 Confidential, *Submission SR 21*, 19 February 2009.

60 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

61 Community and Public Sector Union Members Secrecy Forum, *Consultation*, Canberra, 3 February 2009.

employees to be trained about broader ethics and values in relation to government information handling, in order to instil a greater culture of transparency.

### **ALRC's views**

15.56 Training and development programs are an essential tool for Australian Government agencies to foster compliance by employees and others with their information-handling regime. In order for employees to operate in accordance with secrecy and other information-handling obligations, they must first understand the scope of these obligations and the purpose that they serve. The ALRC proposes that Australian Government agencies develop and administer training and development programs for their employees about their information-handling obligations.

15.57 A number of features should be incorporated in such programs. First, agencies should ensure that they deliver programs that are relevant to the roles of participants. In particular, the ALRC anticipates that this would involve information-handling practices that employees are likely to encounter on a day-to-day basis and avenues for assistance in the case of unusual events.

15.58 Training and development programs should be conducted on induction and at regular intervals thereafter. Ensuring that training takes place throughout an employee's career has the benefit both of refreshing the information imparted in previous training programs, and enabling new obligations to be considered. For example, an employee may incur additional information-handling responsibilities because he or she has attained a higher security classification level or a position of managing staff.

15.59 Finally, training and development programs should also incorporate information on the circumstances in which it is appropriate for an employee to share information and avenues to make public interest disclosures. The need to share information in certain situations is a requirement, for example, under FOI and privacy laws. Ensuring that clear avenues for making public interest disclosures are available to employees and others is a central component of the scheme put forward in the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into whistleblowing protections in the Australian Government.<sup>62</sup> Training and development programs should ensure awareness of such avenues.<sup>63</sup>

---

62 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

63 The Standing Committee recommended that the Commonwealth Ombudsman provide assistance to agencies in implementing the public interest disclosure system, including educational activities to promote awareness of the systems and an anonymous and confidential advice line: *Ibid*, Rec 20.

15.60 The ALRC's proposal is limited to employees of Australian Government agencies. Strategies to foster compliance in the private sector are considered below.

**Proposal 15–4** Australian Government agencies should develop and administer training and development programs for their employees, on induction and at regular intervals thereafter, about the information-handling obligations relevant to their position, including the circumstances in which it is appropriate to share information and the avenues for making public interest disclosures.

## Oaths, affirmations and acknowledgements of secrecy

15.61 Approximately 8% of the secrecy provisions identified by the ALRC—predominantly in laws governing taxation and revenue-protection information—empower a specified person, or persons, to require officers to take an oath or make an affirmation of secrecy.<sup>64</sup> Secrecy obligations may also be included in the oaths of office required for assuming certain public positions, such as the oath taken by Executive Councillors.<sup>65</sup> In addition to conduct covered by these legislative provisions, some agencies have taken administrative action to require officers to sign an acknowledgement of their secrecy obligations.<sup>66</sup>

15.62 Many oaths or affirmations require officers to maintain secrecy ‘in accordance with’ the associated secrecy provision (or words to this effect). Identical conduct is therefore proscribed in both the oath of secrecy and the head secrecy provision, including the same defences and exceptions. For example, the oath and declaration of secrecy set out in the *Income Tax Regulations 1936* (Cth) requires an officer to swear or declare that he or she

will not, either directly or indirectly, *except as permitted under the said section*, and either while I am, or after I cease to be, an officer, make a record or divulge or communicate to any person any information respecting the affairs of another person, disclosed or obtained under the provisions of the *Income Tax Assessment Act 1936*, or of any amendment thereof, or of any Act substituted therefore, or of any previous law of the Commonwealth relating to Income Tax.<sup>67</sup>

64 For example, *Superannuation (Government Co-contribution for Low Income Earners) Act 2003* (Cth) s 53(9); *Termination Payments (Assessment and Collection) Act 1997* (Cth) s 23; *Child Support (Assessment) Act 1989* (Cth) s 150(8); *Fringe Benefits Tax Assessment Act 1986* (Cth) s 5(7); *Student Assistance Act 1973* (Cth) s 12ZU(10); *Income Tax Assessment Act 1936* (Cth) s 16(6). See also: *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 10; *Reserve Bank Act 1959* (Cth) ss 16, 25E.

65 For a discussion of official secrecy provisions that govern Executive Councillors, see P Finn, *Official Information, Integrity in Government Project: Interim Report 1* (1991), 98–100.

66 For example, in 2007, as a part of the distribution of Centrelink's Ethics Resource Kit, Centrelink required all employees to sign a Declaration of Confidentiality: Centrelink, *Annual Report 2006–07* (2007), 40. The Department of Defence also requires employees to sign an official secrecy form acknowledging their obligations: Australian Public Service Commission, *State of the Service Report 2001–02* (2002), 29.

67 *Income Tax Regulations 1936* (Cth) sch 1 (emphasis added).

15.63 The ALRC has heard anecdotally, however, that some Commonwealth employees have been asked to sign oaths that set out substantially more stringent secrecy requirements than those that apply under relevant Commonwealth laws.<sup>68</sup>

15.64 It can be argued that the fact that an officer has taken an oath or affirmation of secrecy is of little or no legal consequence. Professor Enid Campbell commented that:

Nowadays, little or any legal consequence is attached to the fact that a member of an Executive Council, or a Minister, has taken an oath or affirmation of secrecy and has done so by virtue of some legal requirement. The legal significance of the taking of such an oath or affirmation has been considered by courts primarily in the context of the laws of evidence which govern the conduct of judicial proceedings. Rules of common law make it possible for courts to exclude relevant evidence on the ground that its admission would be contrary to the public interest. In recent time the availability of this so-called public interest immunity has been narrowed by the courts and in one of the leading cases before the High Court of Australia—*Sankey v Whitlam* in 1978—Gibbs ACJ firmly rejected the argument that this immunity is automatically attracted when evidence about proceedings before the Federal Executive Council is sought to be adduced, and is so attracted because of the oaths or affirmations taken by members of that Council.<sup>69</sup>

15.65 However, oaths and affirmations of secrecy may have legal consequences where they reinforce the application of other duties of non-disclosure. For example, in setting out the particulars in the case of *Kessing v The Queen*, the New South Wales Court of Criminal Appeal noted that:

On 10 May 2005 the appellant signed documents including an ‘Official Secrets’ form in which he acknowledged his understanding that all official information that he had acquired in the course of his duties for the Commonwealth was not to be published or communicated to any unauthorised person after his service with the Commonwealth. He certified that all information acquired by him in the course of his employment with the Commonwealth had been returned to an appropriate Commonwealth representative.<sup>70</sup>

15.66 Beyond any legal implication, however, oaths and affirmations may carry with them an imprint of moral significance. As one commentator has noted:

There is a particular import, a gravitas, to ... an oath: a message inherent therein that mandates a sense of trust, be it in oneself to fulfill the promise made or, if we are observing the oath or benefiting from its guarantee, in the oath-taker to do the same.<sup>71</sup>

---

68 This was a topic of conversation at the open forum that the ALRC held with members of the CPSU: Community and Public Sector Union Members Secrecy Forum, *Consultation*, Canberra, 3 February 2009.

69 E Campbell, ‘Oaths and Affirmations of Public Office’ (1999) 25(1) *Monash University Law Review* 132, 150. In *Sankey v Whitlam*, Gibbs ACJ commented that ‘the fact that members of the Executive Council are required to take a binding oath of secrecy does not assist the argument that the production of state papers cannot be compelled’. Any obligation must be ‘binding in law and not merely morals’: *Sankey v Whitlam* (1978) 142 CLR 1, 42.

70 *Kessing v The Queen* [2008] NSWCCA 310, [10].

71 N Farid, ‘Oath and Affirmation in the Court: Thoughts on the Power of a Sworn Promise’ (2006) 40 *New England Law Review* 555, 556. See also J McGinness, ‘Secrecy Provisions in Commonwealth Legislation’ (1990) 19 *Federal Law Review* 49, 74, which argues that oaths of secrecy reinforce an ‘atmosphere of unnecessary secrecy’.

## Submissions and consultations

15.67 In IP 34, the ALRC asked what role oaths and affirmations of secrecy play in protecting Commonwealth information, and whether such oaths or affirmations should be retained.<sup>72</sup>

15.68 Stakeholders that commented on this issue unanimously agreed that although oaths and declarations of secrecy may have little legal consequence, they play an important role in reminding staff of their obligations of secrecy. As stated by the Department of Human Services, having employees and contracted service providers sign deeds of confidentiality

reinforces the importance the agency places on the proper management of information it handles and personalises the employee or individual service provider's obligations.<sup>73</sup>

15.69 The concept of personalising information-handling obligations was also evident in other submissions. For example, the Commonwealth Ombudsman submitted that, although it has not been its practice to require staff to swear an oath of office, the approach may have merit as a way of communicating to staff their duties and responsibilities.<sup>74</sup> Liberty Victoria advised that 'whilst the breach of oaths, affirmations or acknowledgements of secrecy may have little legal consequence, they remain an important psychological tool'.<sup>75</sup>

15.70 The AGD commented that, although failure to comply with an oath or affirmation of secrecy is not of itself a criminal offence, the actions that amount to the breach may attract criminal liability. The making of an oath 'enables the legal consequences and duties imposed by secrecy provisions to be presented to Commonwealth officers for their personal acknowledgement and acceptance'. The AGD also noted that courts have taken the signing of an oath of secrecy into account as evidence of the existence of a duty of non-disclosure in accordance with s 70 of the *Crimes Act 1914* (Cth), as seen in the *Kessing* case.<sup>76</sup>

## ALRC's views

15.71 Elsewhere in this Discussion Paper, the ALRC considers the need for individuals subject to secrecy obligations to accept the personal nature of these responsibilities.<sup>77</sup> The strong moral significance accorded to oaths and affirmations of

---

72 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–2.

73 Department of Human Services, *Submission SR 26*, 20 February 2009. See also Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24*, 19 February 2009; The Treasury, *Submission SR 22*, 19 February 2009; Australian Taxation Office, *Submission SR 13*, 16 February 2009.

74 Commonwealth Ombudsman, *Submission SR 20*, 19 February 2009.

75 Liberty Victoria, *Submission SR 19*, 18 February 2009.

76 Attorney-General's Department, *Submission SR 36*, 6 March 2009, referring to *Kessing v The Queen* [2008] NSWCCA 310.

77 See, eg, the discussion of former Commonwealth employees and contracted service providers in Ch 14.

secrecy means that they could play a valuable role in reinforcing this personal responsibility. However, their very gravitas means that, if oaths or affirmations are framed more broadly than the underlying legal obligations, those who enter into them may be inhibited from engaging in lawful information sharing.

15.72 In the ALRC's view, the decision whether or not to administer an oath or affirmation of secrecy should remain at the discretion of the relevant Australian Government agency, in accordance with any legislative provision. However, where an agency decides to administer such an oath or declaration, the agency should ensure that it accurately reflects the requirements under relevant Commonwealth secrecy laws. In particular, the ALRC is concerned about the potential for oaths and affirmations to be broader or more onerous than the secrecy laws on which they are based.

**Proposal 15–5** Any Australian Government agency that administers oaths, affirmations or declarations of secrecy should ensure that these properly reflect what is required under relevant Commonwealth secrecy laws.

## Information and communication technology systems

15.73 The capacity for Commonwealth officers to handle information effectively may depend upon the availability of suitable infrastructure—in particular, ICT systems. Commonwealth officers have identified the improvement of the capacity of ICT infrastructure to support information sharing—particularly secure or confidential information—as a key factor in improving their agency's ability to collaborate with other agencies.<sup>78</sup>

15.74 ICT systems, such as access controls, can lessen the opportunity for inadvertent or deliberate non-compliance on the part of Commonwealth officers. Centrelink, for example, has implemented a 'Deny Access Facility' (DAF), which protects information about the location of certain high-risk clients. Only designated Centrelink officers are able to access DAF records. This limits the potential for the computer records of DAF clients to be accessed inappropriately by Centrelink staff, either inadvertently or by reason of a deliberate breach.<sup>79</sup> Other ICT systems, such as audit control mechanisms, may deter deliberate breaches by Commonwealth officers by facilitating the enforcement of secrecy obligations by Australian Government agencies.

15.75 Effective ICT systems may also promote information-sharing by standardising information-handling practices that may otherwise be contentious or dependent on the favourable exercise of individual discretion. By way of illustration, CrimTrac's National Criminal Investigation DNA Database (NCIDD) provides police with access

<sup>78</sup> Australian Public Service Commission, *State of the Service Report 2006–07* (2007), 241.

<sup>79</sup> Australian Government Child Support Agency and Centrelink, *Protocol Governing the Disclosure of Information Between the Child Support Agency and Centrelink 1 October 2006–30 September 2008*, 4.

to what is effectively a national DNA database, with the capacity to conduct automated intra- and inter-jurisdictional DNA profile-matching. NCIDD has been designed to ensure that only links that comply with Commonwealth, state and territory legislative requirements are available for review. Access is user-based, with data security processes in place to manage and audit such access.<sup>80</sup>

15.76 Where adequate ICT systems are not available, the protection of Commonwealth information can be compromised.<sup>81</sup> For example, as noted in Chapter 3, concerns have been raised about the capacity for ATO officers seconded to law enforcement agencies to have access to the computer systems of both agencies, and, consequently, the potential for unauthorised data matching activities.<sup>82</sup>

### Submissions and consultations

15.77 In IP 34, the ALRC asked about the effectiveness of Australian Government ICT systems in protecting Commonwealth information.<sup>83</sup>

15.78 Law enforcement agencies, in particular, highlighted the important role that ICT systems play in protecting official information. For example, AUSTRAC advised that it uses a ‘sophisticated and secure electronic system’ to collect, analyse and disseminate financial intelligence, including access controls that prevent a designated agency from accessing certain types of information without the appropriate authority; the capacity to audit an agency’s access to AUSTRAC information; and a secure international web-based system for the exchange of information overseas.<sup>84</sup> The AFP noted that it has located reminders about secrecy requirements throughout its intranet where sensitive information is stored.<sup>85</sup> The Australian Commission for Law Enforcement Integrity (ACLEI) submitted that law enforcement agencies usually have in place well-developed ICT systems, and attach a high degree of importance to implementing and maintaining these controls.<sup>86</sup>

15.79 Australian Government agencies in other functional areas also made submissions about how they use ICT systems to protect their information. The ABS noted that it tightly controls access to its ICT systems. ABS employees can only access those sensitive databases that they need in order to perform their duties, and the ABS conducts regular audits of access.<sup>87</sup> The AGD also advised that it had the capacity to ‘lock down’ information to certain persons on a need-to-know basis.<sup>88</sup>

80 CrimTrac, *Annual Report 2006–07* (2007), 18–21.

81 See, eg, comments in PricewaterhouseCoopers, *Australian Taxation Office—Information Security Practices Review Version 2.0* (2008).

82 P Durbin, ‘ATO lashed over privacy breaches’, *Australian Financial Review*, 23 April 2009, 1.

83 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–3(c).

84 Australian Transaction Reports and Analysis Centre, *Submission SR 31*, 2 March 2009.

85 Australian Federal Police, *Submission SR 33*, 3 March 2009.

86 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

87 Australian Bureau of Statistics, *Submission SR 28*, 24 March 2009.

88 Attorney-General’s Department, *Submission SR 36*, 6 March 2009.

### **ALRC's views**

15.80 A diverse array of ICT strategies is used by Australian Government agencies to protect official information. Most commonly, these involve: (a) access controls to prevent employees and others from deliberately or inadvertently gaining access to unnecessary or sensitive information; and (b) audit mechanisms, to log who has gained access to particular files. Some agencies also employ ICT strategies to standardise information-sharing practices by their employees and, in this way, promote the sharing of information in appropriate circumstances.

15.81 The ALRC agrees that ICT strategies can assist Commonwealth employees and others to comply with their obligations of secrecy, and other information-handling, responsibilities. The ALRC proposes that Australian Government agencies should implement protective ICT systems—in particular, access controls and audit mechanisms.

**Proposal 15–6** Australian Government agencies should put in place and maintain information and communication technology systems to facilitate the secure and convenient handling of Commonwealth information, including access controls and audit mechanisms.

### **Avenues for employee queries and concerns**

15.82 As noted above, the *APS Values and Code of Conduct in Practice*, issued by the APSC, suggests that agencies may give a direction to their employees requiring them to seek advice if they are unsure about whether to disclose information.<sup>89</sup> This advice will usually come from an employee’s supervisor.<sup>90</sup> Agencies may establish additional frameworks for an employee to raise queries or concerns about his or her obligations of secrecy.

15.83 The ATO, for example, has instituted a national ATO Privacy Network, comprising members of each of the agency’s business sections. The Network is intended to be the first point of contact to assist employees to resolve privacy and secrecy issues. Network members are also responsible for receiving and reporting complaints about breaches of privacy and secrecy provisions. The ATO directs

<sup>89</sup> Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <[www.apsc.gov.au](http://www.apsc.gov.au)> at 23 September 2008, ch 3.

<sup>90</sup> The influence of supervisors in establishing an agency’s information-handling culture was recognised in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995). The ALRC recommended that the performance agreements of all senior officers should include a requirement to ensure efficient and effective practices and performance in respect of access to government-held information, including FOI requests: Rec 8.

employees to the ATO Legal Services Branch where they may seek further advice or assistance.<sup>91</sup>

15.84 Another option to deal with secrecy queries or concerns is through a program to provide employees with ethics advice more generally. One such strategy is the APSC Ethics Advisory Service that was launched on 6 May 2009.<sup>92</sup> The service will provide advice and resources for applying and interpreting the APS Values and Code of Conduct. Among other initiatives, the service includes an anonymous call and email centre for APS employees to seek advice on ethical issues, including their secrecy obligations under the Code of Conduct.<sup>93</sup> In other situations, an agency may have in place arrangements to provide its employees with ethics advice in a manner that is tailored to the agency's specific circumstances.<sup>94</sup>

15.85 Finally, an employee who has a concern about secrecy obligations may be able to raise it with one or more integrity agencies, such as the Public Service and Merit Protection Commissioners and the Commonwealth Ombudsman.

### ALRC's views

15.86 Providing Commonwealth employees with avenues to raise queries and explore concerns about secrecy laws may help promote effective information handling in Australian Government agencies in two ways. First, where a Commonwealth employee has a ready source of advice about the application of an agency's information-handling policy, there will be a decreased risk of misunderstanding and consequent inadvertent breach of secrecy obligations. Further, to the extent that a deliberate breach is motivated by an employee's desire to feel as though his or her views have been 'heard' by an agency, providing the employee with an avenue to raise concerns may lessen his or her dissatisfaction or disgruntlement.

15.87 The ALRC proposes that Australian Government agencies should develop information-handling policies, which must include, among other information, avenues for an employee to raise queries or concerns.<sup>95</sup> In the ALRC's view, this proposal adequately deals with the need for Australian Government agencies to provide their employees with avenues to seek advice or raise concerns about secrecy obligations. There is no need to specify a particular system that agencies must institute. As long as

91 Australian Taxation Office, *ATO Practice Statement: Secrecy and Privacy Obligations*, PS CM 2004/07 (2004), 4.

92 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <<http://www.smos.gov.au/speeches>> at 6 May 2009.

93 Ibid. See also Australian Public Service Commission, *Introducing the Ethics Advisory Service* (2009) <[www.apsc.gov.au](http://www.apsc.gov.au)> at 8 May 2009.

94 For example, the QCMC advised the ALRC that the Queensland Police Service operates an internal peer support scheme, which provides members with the opportunity to raise issues of concern. The QCMC noted that one of the benefits of this system is the capacity of the peer support officer to reassure the member that steps will be taken to address his or her concern: Crime and Misconduct Commission Queensland, *Consultation*, Brisbane, 20 February 2009.

95 Proposal 15–1.

a clear pathway is provided, it is reasonable for an agency to have a broad discretion as to the manner in which it satisfies this obligation, depending, for example, on the agency's structure and functions, and any related initiatives that it has in place. APS employees—who make up a significant proportion of Commonwealth employees—will also be able to have many of their secrecy queries or concerns addressed through the APSC Ethics Advisory Service.

15.88 The avenues for queries and concerns that are developed by Australian Government agencies will be supplemented by the broader oversight role provided by independent integrity agencies. The operation of integrity agencies for the Australian Government is discussed below.

### **Fostering effective information handling at the agency level**

15.89 A common theme of this Discussion Paper is the personal nature of secrecy obligations and how Commonwealth officers and others who gain access to official information can be held responsible for unauthorised disclosure—for example, through administrative and criminal secrecy obligations and associated penalties. This chapter also focuses on strategies that Australian Government agencies may implement to promote effective information handling by individuals.

15.90 Individual compliance, however, depends upon the practices and processes of Australian Government agencies. For example, one of the risk factors identified by the QCMC for the unauthorised disclosure of information by individuals is a failure by the employing agency to consistently condemn such disclosures. Agency culture may also play a role in determining which breaches are discovered, investigated, and enforced at the administrative level, or referred for prosecution. A further issue, therefore, is how a culture of effective information handling can be fostered at the agency level.

15.91 The following section of this chapter describes the independent oversight mechanisms that apply to the practices and processes of Australian Government agencies. It goes on to consider whether any reforms are necessary in the specific context of the application of secrecy laws.

#### **Commonwealth Ombudsman**

15.92 The Commonwealth Ombudsman is an independent statutory officer, with the function of investigating the administrative actions of Australian Government officers and agencies, either on receipt of a complaint or on the Ombudsman's own motion.<sup>96</sup> This potentially includes a range of agency practices for protecting Commonwealth

---

<sup>96</sup> *Ombudsman Act 1976* (Cth) s 5. The Ombudsman has additional responsibilities in his or her associated role as the Defence Force Ombudsman; Law Enforcement Ombudsman; Immigration Ombudsman; Postal Industry Ombudsman; and Taxation Ombudsman.

information—for instance, a decision by an agency or officer to disclose, or not disclose, information to a third party.<sup>97</sup>

15.93 After completing an investigation, the Ombudsman must make a report to the relevant agency or authority, including recommendations for change, where he or she is of the opinion:

- (a) that the action:
  - (i) appears to have been contrary to law;
  - (ii) was unreasonable, unjust, oppressive or improperly discriminatory;
  - (iii) was in accordance with a rule of law, a provision of an enactment or a practice but the rule, provision or practice is or may be unreasonable, unjust, oppressive or improperly discriminatory;
  - (iv) was based either wholly or partly on a mistake of law or of fact; or
  - (v) was otherwise, in all the circumstances, wrong;
- (b) that, in the course of the taking of the action, a discretionary power had been exercised for an improper purpose or on irrelevant grounds; or
- (c) in a case where the action comprised or included a decision to exercise a discretionary power in a particular manner or to refuse to exercise such a power:
  - (i) that irrelevant considerations were taken into account, or that there was a failure to take relevant considerations into account, in the course of reaching the decision to exercise the power in that manner or to refuse to exercise the power, as the case may be; or
  - (ii) that the complainant in respect of the investigation or some other person should have been furnished, but was not furnished, with particulars of the reasons for deciding to exercise the power in that manner or to refuse to exercise the power, as the case may be.<sup>98</sup>

15.94 The Ombudsman has no power to implement the conclusions of his or her investigation. However, if appropriate action is not taken, the Ombudsman can make a further report to the Prime Minister.<sup>99</sup> The Ombudsman also must file annual reports that are tabled in both Houses of Parliament.<sup>100</sup>

### Australian Public Service and Merit Protection Commissioners

15.95 The *Public Service Act* establishes the role of the APS Commissioner, whose functions include evaluating the extent to which agencies incorporate and uphold the

---

97 Ibid s 5(2)(d), however, expressly prevents the Ombudsman from investigating employment actions (for example, a penalty for a determined breach of the APS Code of Conduct) taken in respect of APS employees.

98 Ibid s 15(1).

99 Ibid s 16.

100 Ibid s 19.

APS Values; and the adequacy of systems and procedures in agencies for ensuring compliance with the APS Code of Conduct.<sup>101</sup>

15.96 Under s 44 of the Act, the Commissioner is required to prepare a report to the Prime Minister, for presentation to Parliament, on the state of the APS during the preceding financial year.<sup>102</sup> Every year the APS Commissioner sends a questionnaire to each agency seeking information on which to base the report.

15.97 In addition, the APS Commissioner will report annually to Parliament on information collected by the Ethics Advisory Service call centre, including on emerging ethical issues and any action that might be needed to strengthen understanding of the APS Values and Code of Conduct.<sup>103</sup>

15.98 The *Public Service Act* also establishes the role of the Merit Protection Commissioner (MPC).<sup>104</sup> The functions of the MPC include reviewing APS actions that relate to the employment of an APS employee and reporting on the results of such inquiries.<sup>105</sup> Recommendations made by the MPC are not legally binding; however, if the MPC is not satisfied with an agency's response to recommendations, he or she may, after consulting with the responsible minister, give a report on the matter to the minister of the responsible agency and to either or both of the Prime Minister and the Presiding Officers, for presentation to Parliament.<sup>106</sup> The responsible minister also may request that the MPC conduct an inquiry into an action by an agency head or another APS employee in relation to an APS employee's employment.<sup>107</sup>

### Australian National Audit Office

15.99 Under the *Auditor-General Act 1997* (Cth), the Auditor-General—supported by the Australian National Audit Office (ANAO)—is responsible for providing auditing services to the Parliament and public sector entities. The ANAO provides the Parliament with an independent assessment of selected areas of public administration, and assurance about public sector financial reporting, administration, risk management and accountability. This function is primarily fulfilled by conducting performance and financial statement audits.<sup>108</sup> The ANAO has conducted a series of audits of the

---

101 *Public Service Act 1999* (Cth) s 41(1)(a), (b).

102 Ibid s 44(3).

103 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <<http://www.smos.gov.au/speeches>> at 6 May 2009. In exceptional cases, the APS Commissioner may also refer issues to the agency head or—where claims of a serious nature or involving imminent risk are identified—to the AFP: Australian Public Service Commission, *Ethics Advisory Service Client Service Charter* (2009) <[www.apsc.gov.au](http://www.apsc.gov.au)> at 7 May 2009.

104 *Public Service Act 1999* (Cth) pt 6.

105 Ibid s 33.

106 Ibid s 33(5), (6).

107 Ibid s 50.

108 Australian National Audit Office, *About Us* (2006) <[www.anoa.gov.au/director/aboutus.cfm](http://www.anoa.gov.au/director/aboutus.cfm)> at 5 September 2008.

policies and practices used by Commonwealth agencies to protect their resources, including Commonwealth information.<sup>109</sup>

### Information Commissioner

15.100 As a part of its anticipated reforms to FOI laws and practices, the Australian Government is proposing to establish an Office of the Information Commissioner. The proposed functions of the Information Commissioner include:

- (a) to report to the Minister on any matter that relates to the Commonwealth Government's policy and practice with respect to:
  - (i) the collection, use, disclosure, management, administration or storage of, or accessibility to, information held by the Government; and
  - (ii) the systems used, or proposed to be used, for the activities covered by subparagraph (i).<sup>110</sup>

15.101 The Companion Guide to the FOI reform package notes that one of the roles for the Information Commissioner is that he or she

will act as an independent monitor for FOI and will be entrusted with a broad range of functions designed to make the Office of the Information Commissioner both a clearing house for FOI matters and a hub for the promotion of the objects of the Act.<sup>111</sup>

### Overseeing specific sectors

15.102 Some Australian Government agencies, including many that handle highly sensitive Commonwealth information, are subject to more specific oversight mechanisms. These include the AFP, the Australian Intelligence Community (AIC) agencies,<sup>112</sup> the Australian Defence Force (ADF), and the ATO.

#### Australian Federal Police

15.103 The Commonwealth Ombudsman, in his or her role as Law Enforcement Ombudsman, has an enhanced investigatory and inspection role in relation to the AFP. The AFP must notify the Ombudsman of all serious misconduct matters dealt with under the *Australian Federal Police Act 1979* (Cth).<sup>113</sup> The Ombudsman must

109 See, eg, Australian National Audit Office, *Managing Security Issues in Procurement and Contracting*, Audit Report 43 (2007); Australian National Audit Office, *Administration of Security Incidents, Including the Conduct of Security Investigations*, Audit Report 41 (2005); Australian National Audit Office, *Management of Protective Security*, Audit Report 55 (2004); Australian National Audit Office, *Personnel Security—Management of Security Clearances*, Audit Report 22 (2001); Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Audit Report 7 (1999); Australian National Audit Office, *Protective Security*, Audit Report 21 (1997).

110 Information Commissioner Bill 2009—Exposure Draft 2009 (Cth) s 9.

111 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009), 8.

112 The six AIC agencies are the: Australian Security Intelligence Organisation; Australian Secret Intelligence Service; Defence Signals Directorate; Defence Imagery and Geospatial Organisation; Defence Intelligence Organisation; and Office of National Assessments.

113 *Australian Federal Police Act 1979* (Cth) s 40TM.

undertake an annual review of the administration of AFP conduct and practices issues,<sup>114</sup> a copy of which must be provided to both the President of the Senate and the Speaker of the House of Representatives for tabling.<sup>115</sup> Further, the Ombudsman may, at any time, inspect records relating to AFP conduct and practices issues for the purposes of conducting an ad hoc review of the administration of AFP conduct and practices issues.<sup>116</sup>

15.104 The Law Enforcement Integrity Commissioner is responsible for preventing, detecting and investigating serious and systemic corruption issues in the AFP and the Australian Crime Commission.<sup>117</sup> The jurisdiction of the Integrity Commissioner potentially could be invoked, for example, where unauthorised handling of Commonwealth information is associated with financial gain on the part of an officer.

#### *Australian Intelligence Community*

15.105 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office holder who reviews the activities of the agencies which collectively comprise the AIC. The IGIS provides independent assurance that the AIC agencies:

- conduct their activities within the law;
- behave with propriety;
- comply with ministerial guidelines and directives; and
- have regard to human rights.<sup>118</sup>

15.106 The IGIS considers complaints or requests from ministers in relation to the actions of AIC agencies. Investigations also can be initiated by his or her own motion. In undertaking inquiries, the IGIS has investigative powers akin to those of a Royal Commission. Where the IGIS completes an inquiry, he or she must provide a report, including any conclusions and recommendations, to the head of the relevant agency and to the responsible minister.<sup>119</sup> The agency head must advise the IGIS of any action taken in response to the inquiry. Where the IGIS is of the view that such action is inadequate or inappropriate, he or she may discuss the matter with the responsible minister and prepare a report, a copy of which is provided to the Prime Minister.<sup>120</sup>

---

114 Ibid pt V div 7.

115 Ibid s 40XD.

116 Ibid s 40XB.

117 *Law Enforcement Integrity Commissioner Act 2006* (Cth).

118 Inspector-General of Intelligence and Security, *About IGIS* (2008) <[www.igis.gov.au/about.cfm](http://www.igis.gov.au/about.cfm)> at 7 October 2008.

119 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 22.

120 Ibid s 24.

15.107 Additional oversight of the AIC is provided by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The PJCIS is required, under s 29(1)(a) of the *Intelligence Services Act 1982* (Cth), to conduct an annual review of the administration, expenditure and financial statements of the AIC. The PJCIS does not conduct inquiries into individual complaints about the AIC agencies' activities.

#### **Australian Defence Force**

15.108 The Inspector-General of the ADF (IGADF) is a statutory position introduced in 2005 to oversee the ADF military justice system.<sup>121</sup> The principal functions of the IGADF are:

inquiring into complaints about the military justice system that cannot be dealt with through the usual channels, conducting an ongoing scrutiny of the effectiveness of the system through a program of rolling audits of military justice arrangements at unit level, and analysing a broad spectrum of military justice statistical data.<sup>122</sup>

15.109 The IGADF does not have the power to implement measures arising out of his or her investigations. Rather, the IGADF may report the outcome of inquiries to the Chief of the ADF, an official in the Department of Defence, a member of the ADF or another person affected by the inquiry.<sup>123</sup> The Department of Defence's annual report also includes a section on the operation of the Office of the IGADF.

15.110 Additional oversight of the ADF is provided by the Defence Force Ombudsman (DFO), another office of the Commonwealth Ombudsman. The DFO can investigate administrative actions related to or arising out of a person's service in the ADF, either following receipt of a complaint or on the DFO's own motion.<sup>124</sup> In general, before the DFO will investigate a complaint from an ADF member, the member must first have exhausted internal grievance mechanisms. The DFO is not authorised to investigate disciplinary action taken against an ADF member.<sup>125</sup>

#### **Australian Taxation Office**

15.111 The Inspector-General of Taxation is an independent statutory office holder who reviews systemic tax administration issues. Section 7 of the *Inspector-General of Taxation Act 2003* (Cth) sets out the functions of the Inspector-General as being:

- (a) to review:
  - (i) systems established by the Australian Taxation Office to administer the tax laws, including systems for dealing or communicating with the public generally, or with particular people or organisations, in relation to the administration of the tax laws; and

121 *Defence Act 1903* (Cth) pt VIIIB. The position of the IGADF was introduced in the *Defence Legislation Amendment Act (No 2) 2005* (Cth).

122 Australian Government Department of Defence, *Annual Report 2006–07* (2007), 156.

123 *Defence (Inquiry) Regulations 1985* (Cth) reg 102(3).

124 *Ombudsman Act 1976* (Cth) s 19C(2), (3).

125 *Ibid* s 19C(5)(d).

- (ii) systems established by tax laws, but only to the extent that the systems deal with administrative matters; and
- (b) to report on those reviews, setting out:
  - (i) the subject and outcome of the review; and
  - (ii) any recommendations that the Inspector-General thinks appropriate concerning how the system reviewed could be improved.

15.112 Where the Inspector-General, in the course of his or her review, forms the opinion that a tax official has engaged in misconduct, the Inspector-General must report the evidence to the Commissioner of Taxation.<sup>126</sup>

### **Submissions and consultations**

15.113 In IP 34, the ALRC asked about the effectiveness of the mechanisms for monitoring and overseeing the application by Australian Government agencies of Commonwealth secrecy laws.<sup>127</sup>

15.114 The AFP advised that its standards are overseen by the Commonwealth Law Enforcement Ombudsman and ACLEI.<sup>128</sup> The AIC submitted that there are extensive oversight mechanisms in place relating to the intelligence agencies—in particular, the role of the IGIS. These arrangements ensure that there is transparency in the protections afforded to the AIC.<sup>129</sup> The Australian Prudential Regulatory Authority advised that its mechanisms were ‘as effective as is practicable’.<sup>130</sup> ASIC agreed that, in its ‘limited experience’, these mechanisms appear effective.<sup>131</sup>

15.115 A contrasting view was put forward by PIAC, which submitted that current arrangements relating to the Ombudsman and the IGIS are inadequate, so far as they are limited to the making of a report to the Prime Minister.<sup>132</sup> Whistleblowers Australia expressed the view that the APSC has been ineffective in overseeing the application of Commonwealth secrecy laws and submitted that its powers should be transferred to the ACLEI.<sup>133</sup>

15.116 Liberty Victoria commented on the importance of independent and effective oversight bodies empowered to investigate and report on alleged misconduct by

---

126 *Inspector-General of Taxation Act 2003* (Cth) s 38. Where the Inspector-General suspects misconduct on the part of the Commissioner of Taxation, the matter is reported to the Minister: s 38(c).

127 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–10.

128 Australian Federal Police, *Submission SR 33*, 3 March 2009.

129 Australian Intelligence Community, *Submission SR 37*, 6 March 2009.

130 Australian Prudential Regulation Authority, *Submission SR 12*, 13 February 2009.

131 Australian Securities & Investments Commission, *Submission SR 41*, 17 March 2009.

132 Public Interest Advocacy Centre Ltd, *Submission SR 38*, 9 March 2009.

133 Whistleblowers Australia, *Submission SR 40*, 10 March 2009.

Commonwealth officers. It submitted that every agency or department should fall within the purview of at least one such body.<sup>134</sup>

15.117 The AGD noted that monitoring and overseeing the application of secrecy laws is not the primary role of bodies such as the Ombudsman and the APS Commissioner, although they may be able to consider particular matters following specific complaints.<sup>135</sup>

15.118 Some stakeholders made submissions on the importance of having available avenues for whistleblowing.<sup>136</sup> James Renwick, for example, stated that there should be a clear mechanism for the public servant who genuinely believes that a government is going to behave unlawfully to report that information.<sup>137</sup> The CPSU advised that its members strongly supported an independent body where employees could raise complaints and allegations without breaching secrecy provisions or employment duties.<sup>138</sup> ACLEI considered that the capacity for whistleblowers to bring information to it directly for independent assessment and investigation is an important part of its role.<sup>139</sup> Participants in the national secrecy phone-in advised of the lack of support for officers wanting to report misconduct. One caller stated that officers feel they have no place to go to report misconduct with confidence that something will be done about it.<sup>140</sup>

### ALRC's view

15.119 Australian Government agencies are subject to a number of independent oversight mechanisms, including the Commonwealth Ombudsman, the APS Commissioner, MPC and the ANAO. For many of the agencies that handle highly sensitive Commonwealth information, such as the AIC, specific oversight mechanisms have been established. For the reasons set out below, the ALRC considers this provides an adequate framework to promote effective information handling in Australian Government agencies.

15.120 The independent oversight mechanisms that currently apply to the Australian Government have not been established for the primary purpose of ensuring compliance with information-handling obligations. Many of their functions, however, are potentially applicable in this context. Hypothetically, for example, the Commonwealth Ombudsman could investigate the systemic leaking of information by Commonwealth officers. The APS Commissioner could report on an APS agency's administrative disciplinary system, where its operation, for example, was inadequate to promote

134 Liberty Victoria, *Submission SR 19*, 18 February 2009. Liberty Victoria also noted the ongoing need for judicial oversight, including, where necessary, access by the judiciary to classified information.

135 Attorney-General's Department, *Submission SR 36*, 6 March 2009.

136 Public interest disclosure, or 'whistleblowing', is discussed in Ch 9.

137 J Renwick, *Submission SR 02*, 11 December 2008.

138 Community and Public Sector Union, *Submission SR 32*, 2 March 2009.

139 Australian Commission for Law Enforcement Integrity, *Submission SR 18*, 18 February 2009.

140 *Secrecy Phone-In*, 11–12 February 2009.

compliance by employees with their secrecy obligations under the APS Code of Conduct.

15.121 The proposed Information Commissioner will supplement the functions of the general integrity agencies. The Commissioner's functions are expected to include reporting to the responsible minister on Australian Government policy and practice with respect to 'the collection, use, disclosure, management, administration or storage of, or accessibility to, information held by the Government' and the systems used for these activities. These functions encompass issues concerning the application of secrecy laws in Australian Government agencies—including, for example, agency information-handling policies and ICT systems for information sharing. The Commissioner has also been given an important role in education and training.

15.122 A determination of breach of an administrative secrecy obligation, and any penalty imposed, by an Australian Government agency may also be subject to judicial review. As noted in Chapter 13, an APS employee may seek merits review of most agency-level secrecy determinations by applying to the MPC or, where appropriate, the Australian Industrial Relations Commission. In accordance with Proposal 13–1, Australian Government agencies that employ persons other than under the *Public Service Act* should institute a merits review process, to the extent that this is consistent with the agency's functions and structure.

15.123 At this stage, the ALRC is not proposing reforms concerning the whistleblowing avenues available to those who have access to Commonwealth information. This issue was comprehensively canvassed by the House of Representatives Standing Committee on Legal and Constitutional Affairs in its 2009 report on whistleblowing protections in the Australian Government.<sup>141</sup> The interaction between this Inquiry and recommendations in the Standing Committee's report is discussed in detail in Chapter 9.

## **Fostering effective information handling in the private sector**

15.124 Previous sections of this chapter have considered a variety of strategies that have been put in place by Australian Government agencies to promote effective information-handling by employees, including, for example, information-handling policies, training and development programs and protective ICT systems. However, where the person accessing information is not in an employment relationship with the Commonwealth, these strategies may not be available. In particular, the ALRC questions whether employees of contracted service providers are always aware of their potential criminal liability under secrecy laws.

---

<sup>141</sup> Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009).

15.125 As discussed in Chapter 14, extensive Commonwealth information may be accessed by private sector contracted service providers. In some situations, the unauthorised disclosure of this information will satisfy the harm requirements for criminal liability under the general secrecy offence or a more specific secrecy offence. In Chapter 8, the ALRC considers which parties should be covered by the general secrecy offence. The ALRC proposes that the offence should extend to ‘individuals and entities who are contracted service providers for a Commonwealth contract’.<sup>142</sup> Specific secrecy offences might also apply to employees of contracted service providers.

15.126 Attaching criminal liability to the unauthorised disclosure of information is a unique incidence of government information. No such liability results from the disclosure of other confidential information, such as information obtained under a contract with another private sector organisation. This can be distinguished from obligations of non-disclosure that arise under the general law, including contractual obligations and the equitable duty of confidence. These obligations arise regardless of whether the information originated from government or the private sector.

15.127 If employees of contracted service providers are unaware of the liability associated with the unauthorised disclosure of Commonwealth information, the criminal offences will have no deterrent effect. Further, it is not desirable to impose criminal sanctions on a person who was unaware of his or her potential liability. Therefore, the ALRC is proposing that private sector organisations that perform services for or on behalf of the Australian Government should take steps to make their staff aware of their obligations of secrecy—and, in particular, any relevant criminal offences.

**Proposal 15–7** Private sector organisations that perform services for or on behalf of the Australian Government under contract should take steps to ensure that all employees who access Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal, civil or administrative liability could result.

142 Proposal 8–1.



## **Appendix 1. List of Submissions**

---

<b>Name</b>	<b>Submission Number</b>	<b>Date</b>
Attorney-General's Department	SR 36	6 March 2009
Australia's Right to Know	SR 35	6 March 2009
Australian Transaction Reports and Analysis Centre	SR 31	2 March 2009
Australian Bureau of Statistics	SR 28	24 March 2009
Australian Commission for Law Enforcement Integrity	SR 18	18 February 2009
Australian Competition & Consumer Commission	SR 11	12 February 2009
Australian Federal Police	SR 33	3 March 2009
Australian Intelligence Community	SR 37	6 March 2009
Australian Press Council	SR 16	18 February 2009
Australian Prudential Regulation Authority	SR 12	13 February 2009
Australian Securities & Investments Commission	SR 41	17 March 2009
Australian Taxation Office	SR 13	16 February 2009
A J Brown	SR 44	18 May 2009
J Butterworth	SR 07	9 February 2009
B Calcutt	SR 10	11 February 2009

---

Clerk of the Senate	SR 03	23 January 2009
Commonwealth Director of Public Prosecutions	SR 17	18 February 2009
Commonwealth Ombudsman	SR 20	19 February 2009
Confidential	SR 09	11 February 2009
Confidential	SR 21	19 February 2009
A Chynoweth	SR 06	2 February 2009
Community and Public Sector Union	SR 32	2 March 2009
Department of Climate Change	SR 27	23 February 2009
Department of Education, Employment and Workplace Relations	SR 24	19 February 2009
Department of Families, Housing, Community Services and Indigenous Affairs	SR 45	18 May 2009
Department of Human Services	SR 26	20 February 2009
N Edwards	SR 08	10 February 2009
Fairness in Child Support	SR 23	19 February 2009
R Fraser	SR 42	23 March 2009
IP Australia	SR 05	4 February 2009
Jennifer	SR 43	6 March 2009
Law Council of Australia	SR 30	27 February 2009
Liberty Victoria	SR 19	18 February 2009
Media, Entertainment & Arts Alliance	SR 39	10 March 2009
W Mentink	SR 25	20 February 2009
National Archives of Australia	SR 29	23 February 2009

Non-Custodial Parents Party	SR 04	3 February 2009
NSW Young Lawyers Human Rights Committee	SR 34	4 March 2009
Public Interest Advocacy Centre Ltd	SR 38	9 March 2009
J Renwick	SR 02	11 December 2008
N Rogers	SR 01	9 December 2008
Social Security Appeals Tribunal	SR 14	17 February 2009
The Treasury	SR 22	19 February 2009
I Turnbull	SR 15	17 February 2009
Whistleblowers Australia	SR 40	10 March 2009



## **Appendix 2. List of Agencies, Organisations and Individuals Consulted**

---

<i>Name</i>	<i>Location</i>
Australian Bureau of Statistics	Sydney
Australian Electoral Commission	Canberra
Australian Federal Police	Canberra
Australian Government Solicitor	Canberra
Australian Intelligence Community	Canberra
Australian Public Service Commissioner	Canberra
Australian Taxation Office	Canberra
Attorney-General's Department	Canberra
Professor A J Brown	Gold Coast
Centrelink and other Australian Government Agencies	Canberra
Commonwealth Director of Public Prosecutions	Canberra
Community and Public Sector Union	Sydney; Canberra
C Erskine SC	Sydney
Monash University academics	Melbourne
Members of the New South Wales Bar Association	Sydney
Justice H Penfold, Supreme Court of the ACT	Canberra
Queensland Crime and Misconduct Commission	Brisbane
Justice R Refshauge, Supreme Court of the ACT	Canberra
Dr D Solomon	Sydney



## Appendix 3. List of Abbreviations

---

AAT	Administrative Appeals Tribunal
ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACLEI	Australian Commission for Law Enforcement Integrity
ADF	Australian Defence Force
ADJR Act	<i>Administrative Decisions (Judicial Review) Act 1977</i> (Cth)
AEC	Australian Electoral Commission
AFP	Australian Federal Police
AFP Act	<i>Australian Federal Police Act 1979</i> (Cth)
AGD	Australian Government Attorney-General's Department
AGS	Australian Government Solicitor
AIC	Australian Intelligence Community
AIRC	Australian Industrial Relations Commission
ALRC	Australian Law Reform Commission
ALRC 77	Australian Law Reform Commission, <i>Open Government: A Review of the Freedom of Information Act 1982</i> , ALRC 77 (1995)
ALRC 85	Australian Law Reform Commission, <i>Australia's Federal Record: A Review of Archives Act 1983</i> , ALRC 85 (1998)

---

ALRC 95	Australian Law Reform Commission, <i>Principled Regulation: Federal Civil and Administrative Penalties in Australia</i> , ALRC 95 (2002)
ALRC 98	Australian Law Reform Commission, <i>Keeping Secrets: The Protection of Classified and Security Sensitive Information</i> , ALRC 98 (2004)
ALRC 102	Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, <i>Uniform Evidence Law</i> , ALRC 102 (2005)
ALRC 107	Australian Law Reform Commission, <i>Privilege in Perspective—Client Legal Privilege in Federal Investigations</i> ALRC 107 (2007)
ALRC 108	Australian Law Reform Commission, <i>For Your Information: Australian Privacy Law and Practice</i> , ALRC 108 (2008)
AMC	Australian Military Court
AML/CTF Act	<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i> (Cth)
ANAO	Australian National Audit Office
APRA	Australian Prudential Regulation Authority
APRA Act	<i>Australian Prudential Regulation Authority Act 1998</i> (Cth)
APSC	Australian Public Service Commission
APS	Australian Public Service
ARC	Administrative Review Council
ARTKC	Australia's Right to Know Coalition
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	<i>Australian Security Intelligence Organisation Act 1979</i> (Cth)

ASIS	Australian Secret Intelligence Service
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
CAC Act	<i>Commonwealth Authorities and Companies Act 1997</i> (Cth)
CCPM	Case Categorisation and Prioritisation Model
CEO	Chief Executive Officer
CDPP	Commonwealth Director of Public Prosecutions
CO	Commanding Officer
COAG	Council of Australian Governments
CPSU	Community and Public Sector Union
CRS	Commonwealth Rehabilitation Service
DAF	Deny Access Facility
DEEWR	Department of Education, Employment and Workplace Relations
DFD Act	<i>Defence Force Discipline Act 1982</i> (Cth)
DFO	Defence Force Ombudsman
DHS	Department of Human Services
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DPP	Director of Public Prosecutions
DSD	Defence Signals Directorate

---

FMA Act	<i>Financial Management and Accountability Act 1997 (Cth)</i>
FOI	Freedom of Information
FOI Act	<i>Freedom of Information Act 1982 (Cth)</i>
HREOC	Human Rights and Equal Opportunity Commission
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
IGADF	Inspector-General of the Australian Defence Force
IGIS	Inspector-General of Intelligence and Security
ILC	Indigenous Land Corporation
IP 34	Australian Law Reform Commission, Issues Paper, <i>Review of Secrecy Laws</i> (2009)
IPPs	Information Privacy Principles
MOPS Act	<i>Members of Parliament (Staff) Act 1984 (Cth)</i>
MOU	Memorandum of understanding
MPC	Merit Protection Commissioner
NAA	National Archives of Australia
NCIDD	National Criminal Investigation DNA Database
NPPs	National Privacy Principles
NSI	National Security Information
ONA	Office of National Assessments
OPC	Office of Parliamentary Counsel
PIAC	Public Interest Advocacy Centre

PJCIS	Parliamentary Joint Committee on Intelligence and Security
PSM	Australian Government Protective Security Manual
QCMC	Queensland Crime and Misconduct Commission
SSAT	Social Security Appeals Tribunal
TISN	Trusted Information Sharing Network
UK	United Kingdom
UK FOI Act	<i>Freedom of Information Act 2000 (UK)</i>
US	United States



## **Appendix 4. Table of Secrecy Provisions**

---

The first section of this table lists the provisions in Commonwealth legislation that impose secrecy or confidentiality obligations and criminal penalties for breach as identified to date. The second section lists all other provisions that impose such obligations and do not contain express criminal penalties for breach. Some of the latter provisions create obligations, breach of which may lead to criminal penalties under s 70 of the *Crimes Act 1914* (Cth). Provisions that relate only to exceptions to secrecy or confidentiality obligations and other associated matters are not included.

<b>Criminal secrecy offences</b>	
<b>Legislation</b>	<b>Provision</b>
<i>A New Tax System (Australian Business Number) Act 1999</i>	s 30
<i>A New Tax System (Bonuses for Older Australians) Act 1999</i>	s 55
<i>A New Tax System (Family Assistance)(Administration) Act 1999</i>	ss 164; 166(1), (2); 163; 165
<i>A New Tax System (Goods and Services Tax Administration) Act 1999</i>	s 68
<i>Aboriginal and Torres Strait Islander Act 2005</i>	ss 191; 193S; 200A
<i>Aboriginal Land Rights (Northern Territory) Act 1976</i>	s 23E(2), (4)
<i>Age Discrimination Act 2004</i>	s 60
<i>Aged Care Act 1997</i>	ss 86-2; 86-5; 86-6; 86-7
<i>Agricultural and Veterinary Chemicals Code Act 1994</i>	s 162(1), (8), (9)
<i>Agricultural and Veterinary Chemicals Code Regulations 1995</i>	reg 69

**Criminal secrecy offences****Legislation****Provision**

<i>Anti-Money Laundering and Counter-Terrorism Financing Act 2006</i>	ss 121; 122; 123; 127; 128(5), (10); 130; s 131(4)
<i>Auditor-General Act 1997</i>	s 36(1), (3)
<i>AusCheck Act 2007</i>	s 15
<i>Australian Citizenship Act 2007</i>	ss 42; 43
<i>Australian Crime Commission Act 2002</i>	ss 29B(1), (3); 51
<i>Australian Federal Police Act 1979</i>	ss 40ZA; 60A
<i>Australian Hearing Services Act 1991</i>	s 67(8)
<i>Australian Institute of Health and Welfare Act 1987</i>	s 29
<i>Australian Postal Corporation Act 1989</i>	ss 90H; 90LB; 90LE
<i>Australian Prudential Regulation Authority Act 1998</i>	s 56
<i>Australian Securities and Investments Commission Act 2001</i>	s 127(4EA), (4F)
<i>Australian Security Intelligence Organisation Act 1979</i>	ss 18; 34ZS(1), (2); 81; 92(1), (1A)
<i>Australian Sports Anti-Doping Authority Act 2006</i>	ss 71; 72
<i>Australian Trade Commission Act 1985</i>	s 94
<i>Aviation Transport Security Act 2004</i>	s 74
<i>Aviation Transport Security Regulations 2005</i>	regs 2.06; 4.46(2), (3), (4)
<i>Banking Act 1959</i>	ss 11CF; 52E

<b>Criminal secrecy offences</b>	
<b>Legislation</b>	<b>Provision</b>
<i>Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992</i>	s 25
<i>Building and Construction Industry Improvement Act 2005</i>	s 65
<i>Census and Statistics Act 1905</i>	s 19
<i>Chemical Weapons (Prohibition) Act 1994</i>	s 102(2), (3A), (3C)
<i>Child Care Act 1972</i>	ss 12K; 12L; 12Q; 12R; 12S
<i>Child Support (Assessment) Act 1989</i>	ss 150; 150AA
<i>Child Support (Registration and Collection) Act 1988</i>	ss 16; 16AA; 58
<i>Civil Aviation Act 1988</i>	s 32AP(1), (2)
<i>Civil Aviation Regulations 1988</i>	reg 132
<i>Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992</i>	s 14
<i>Commonwealth Electoral Act 1918</i>	ss 91A; 91B(2), (3); 189B(1), (2), (3); 323
<i>Commonwealth Functions (Statutes Review) Act 1981</i>	s 234
<i>Competition Policy Reform (Transitional Provisions) Regulations 1995</i>	reg 6
<i>Comprehensive Nuclear Test-Ban Treaty Act 1998</i>	s 74(2), (4)
<i>Copyright Act 1968</i>	s 203E

<b>Criminal secrecy offences</b>	
<b>Legislation</b>	<b>Provision</b>
<i>Corporations (Aboriginal and Torres Strait Islander) Act 2006</i>	ss 175-10; 183-1; 472-1; 604-15; 604-20
<i>Crimes Act 1914</i>	ss 15XS(1), (2); 23XG; 23YO; 3ZQJ; 3ZQT; 70(1), (2); 79(2), (3), (4), (5), (6); 83
<i>Crimes (Taxation Offences) Act 1980</i>	ss 4(1), (1A), (1AA), (4); sch 1 s 355-5
<i>Criminal Code</i>	ss 91.1(1), (2), (3), (4); 105.41(1), (2), (3), (4A), (5), (6), (7)
<i>Customs Act 1901</i>	s 64ADA
<i>Customs Administration Act 1985</i>	s 16
<i>Dairy Produce Act 1986</i>	s 119(2)(a), (b); sch 2 cl 43
<i>Data-matching Program (Assistance and Tax) Act 1990</i>	s 15
<i>Defence Act 1903</i>	s 73A
<i>Defence Force Discipline Act 1982</i>	ss 16; 58
<i>Defence (Inquiry) Regulations 1985</i>	regs 62; 63
<i>Defence (Special Undertakings) Act 1952</i>	s 9
<i>Dental Benefits Act 2008</i>	ss 34; 43; 44; 45; 46
<i>Designs Act 2003</i>	s 108
<i>Development Allowance Authority Act 1992</i>	s 114
<i>Disability Discrimination Act 1992</i>	s 127
<i>Disability Services Act 1986</i>	s 28
<i>Environment Protection (Alligator Rivers Region) Act 1978</i>	s 31(2), (4)

<b>Criminal secrecy offences</b>	
<b>Legislation</b>	<b>Provision</b>
<i>Environment Protection and Biodiversity Conservation Act 1999</i>	sch 1 cls 51; 53
<i>Epidemiological Studies (Confidentiality) Act 1981</i>	ss 4; 6
<i>Equal Opportunity for Women in the Workplace Act 1999</i>	s 32
<i>Excise Act 1901</i>	s 159
<i>Export Finance and Insurance Corporation Act 1991</i>	s 87(5)
<i>Financial Transaction Reports Act 1988</i>	s 16(5A), (5AA)
<i>First Home Saver Accounts Act 2008</i>	s 70
<i>Fisheries Management Act 1991</i>	sch 1A cl 53
<i>Fisheries Management Regulations 1992</i>	reg 36
<i>Food Standards Australia New Zealand Act 1991</i>	s 114(8)
<i>Fringe Benefits Tax Assessment Act 1986</i>	s 5
<i>Gene Technology Act 2000</i>	s 187(1), (2)
<i>Health Insurance Act 1973</i>	ss 124Y; 130(1), (3B), (3C), (4), (9), (14), (15), (17), (19), (21), (22)
<i>Higher Education Funding Act 1988</i>	s 78(4)
<i>Higher Education Support Act 2003</i>	ss 179-10; 179-35
<i>Human Rights and Equal Opportunity Commission Act 1986</i>	s 49
<i>Income Tax Assessment Act 1936</i>	ss 16; 16A

**Criminal secrecy offences****Legislation****Provision**

<i>Income Tax Assessment Act 1997</i>	s 396-95
<i>Inspector of Transport Security Act 2006</i>	ss 35(7); 36(7), (8); 49(2); 56; 60(5); 63(4), (5); 67; 75
<i>Inspector-General of Intelligence and Security Act 1986</i>	s 34
<i>Inspector-General of Taxation Act 2003</i>	s 37
<i>Insurance Act 1973</i>	s 107
<i>Intelligence Services Act 2001</i>	ss 39; 39A; 40; 41; sch 1 cl 9
<i>International Criminal Court Act 2002</i>	s 92
<i>Law Enforcement Integrity Commissioner Act 2006</i>	ss 90; 92(1), (3), (5); 207
<i>Life Insurance Act 1995</i>	ss 156E; 230E
<i>Maritime Transport and Offshore Facilities Security Act 2003</i>	s 40
<i>Medical Indemnity Act 2002</i>	s 77
<i>Migration Act 1958</i>	ss 261AKD; 336C; 336E; 377; 439
<i>Mutual Assistance in Criminal Matters Act 1987</i>	ss 34V; 43B; 43C
<i>National Blood Authority Act 2003</i>	s 11
<i>National Environment Protection Measures (Implementation) Act 1998</i>	s 36

<b>Criminal secrecy offences</b>	
<b>Legislation</b>	<b>Provision</b>
<i>National Greenhouse and Energy Reporting Act 2007</i>	s 23
<i>National Health Act 1953</i>	ss 135A(1), (4), (9), (13), (14), (16), (18), (20), (21); 135AAA(1), (3), (6), (8)
<i>National Health and Medical Research Council Act 1992</i>	s 80(2), (7), (11)
<i>National Health Security Act 2007</i>	ss 21; 90
<i>National Residue Survey Administration Act 1992</i>	s 11(5)
<i>National Water Commission Act 2004</i>	s 43
<i>Nuclear Non-Proliferation (Safeguards) Act 1987</i>	s 71
<i>Offshore Minerals Act 1994</i>	s 374(1), (2)
<i>Ombudsman Act 1976</i>	s 35(2), (5)
<i>Parliamentary Commission of Inquiry (Repeal) Act 1986</i>	s 7
<i>Parliamentary Privileges Act 1987</i>	s 13
<i>Patents Act 1990</i>	ss 173; 184
<i>Petroleum Resource Rent Tax Assessment Act 1987</i>	ss 17; 18
<i>Pooled Development Funds Act 1992</i>	s 71
<i>Port Statistics Act 1977</i>	s 7
<i>Postal and Telecommunications Commissions (Transitional Provisions) Act 1975</i>	s 37

**Criminal secrecy offences****Legislation****Provision**

<i>Privacy Act 1988</i>	ss 80Q; 96
<i>Private Health Insurance Act 2007</i>	ss 323-1; 323-40; 323-45; 323-50; 323-55
<i>Proceeds of Crime Act 1987</i>	s 74(1), (2)
<i>Proceeds of Crime Act 2002</i>	ss 210(1), (2); 217; 223(1), (2), (3)
<i>Product Grants and Benefits Administration Act 2000</i>	s 47
<i>Productivity Commission Act 1998</i>	s 53
<i>Public Service Regulations 1999</i>	regs 6.3; 7.6
<i>Racial Discrimination Act 1975</i>	s 27F(1)
<i>Referendum (Machinery Provisions) Act 1984</i>	s 116
<i>Renewable Energy (Electricity) Act 2000</i>	s 127
<i>Research Involving Human Embryos Act 2002</i>	s 30(1), (2)
<i>Reserve Bank Act 1959</i>	ss 79A; 79B
<i>Sex Discrimination Act 1984</i>	ss 92; 112
<i>Social Security (Administration) Act 1999</i>	ss 203; 204; 205; 206
<i>Social Welfare Commission (Repeal) Act 1976</i>	s 8
<i>Space Activities Act 1998</i>	s 96
<i>Student Assistance Act 1973</i>	ss 12ZU; 352; 353; 357; 358; 359
<i>Superannuation Contributions Tax (Assessment and Collection) Act 1997</i>	s 32
<i>Superannuation Contributions Tax</i>	s 28

<b>Criminal secrecy offences</b>	
<b>Legislation</b>	<b>Provision</b>
<i>(Members of Constitutionally Protected Superannuation Funds) Assessment and Collection Act 1997</i>	
<i>Superannuation (Government Co-contribution for Low Income Earners) Act 2003</i>	s 53
<i>Superannuation Guarantee (Administration) Act 1992</i>	s 45
<i>Superannuation Industry (Supervision) Act 1993</i>	s 252C
<i>Superannuation (Resolution of Complaints) Act 1993</i>	s 63(2), (3B)
<i>Superannuation (Unclaimed Money and Lost Members) Act 1999</i>	s 32
<i>Surveillance Devices Act 2004</i>	s 45(1), (2)
<i>Taxation Administration Act 1953</i>	ss 3C; 3D; 3E(2), (2B), (5), (6C); 3EA; 3EB; 3EC; 3G(6), (9); 3H(5), (8); 8WB; 8XA; 8XB; 13H; 13J; sch 1 s 355-5
<i>Taxation (Interest on Overpayments and Early Payments) Act 1983</i>	s 8
<i>Telecommunications (Interception and Access) Act 1979</i>	ss 63(1), (2); 133; 182
<i>Termination Payments Tax (Assessment and Collection) Act 1997</i>	s 23
<i>Torres Strait Fisheries Act 1984</i>	sch 2 cls 51; 53
<i>Torres Strait Fisheries Regulations 1985</i>	reg 13
<i>Trade Practices Act 1974</i>	ss 10.89; 95ZP; 95ZQ

**Criminal secrecy offences****Legislation****Provision**

*Transport Safety Investigation Act 2003* ss 26(2)(a), (b); 53(1), (2); 60(1), (2), 60(3)

*Wheat Export Marketing Act 2008* s 74

*Wheat Export Marketing (Repeal and Consequential Amendments) Act 2008* sch 3 item 6

*Witness Protection Act 1994* s 22(1), (2)

*Workplace Relations Act 1996* ss 165; 425(1), (3); 486

**Other secrecy provisions**

<b>Legislation</b>	<b>Provision</b>
<i>A New Tax System (Australian Business Number) Act 1999</i>	s 26
<i>Aged Care Act 1997</i>	ss 62-1; 63-1AA
<i>Air Navigation (Confidential Reporting) Regulations 2006</i>	reg 14
<i>Air Navigation Regulations 1947</i>	reg 12
<i>Airports (Building Control) Regulations 1996</i>	reg 4.03
<i>Airports (Environment Protection) Regulations 1997</i>	reg 10.06
<i>Archives Act 1983</i>	s 30A
<i>Auditor-General Act 1997</i>	s 37
<i>Australian Crime Commission Act 2002</i>	s 9
<i>Australian Federal Police Regulations 1979</i>	regs 12; 13B; 13C
<i>Australian Hearing Services Act 1991</i>	s 67(1)
<i>Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989</i>	s 41
<i>Australian Securities and Investments Commission Act 2001</i>	ss 127(1); 213; 237
<i>Australian Wine and Brandy Corporation (Annual General Meeting of the Industry) Regulations 1999</i>	reg 9
<i>Bankruptcy Regulations 1996</i>	regs 8.05O; 8.32

**Other secrecy provisions**

<b>Legislation</b>	<b>Provision</b>
<i>Building and Construction Industry Improvement Act 2005</i>	s 66
<i>Cadet Forces Regulations 1977</i>	sch 4 cl 5
<i>Census and Statistics Act 1905</i>	ss 12; 13; 19A
<i>Commonwealth Electoral Act 1918</i>	s 90B
<i>Crimes Act 1914</i>	s 23XWO
<i>Designs Act 2003</i>	s 61
<i>Environment Protection and Biodiversity Conservation Act 1999</i>	ss 131AA(4); 133(4); 143(6); 146B(4); 170B; 189B; 251(3); 324R; 341R; 390R
<i>Export Finance and Insurance Corporation Act 1991</i>	s 87(4)
<i>Family Law Act 1975</i>	ss 10D; 10H
<i>Film Licensed Investment Company (Application) Rules 2005</i>	rule 17
<i>Fisheries Administration Act 1991</i>	s 101(6)
<i>Food Standards Australia New Zealand Act 1991</i>	s 114(1)
<i>Health Insurance Regulations 1975</i>	reg 23C(2)(a)
<i>Industry Research and Development Act 1986</i>	s 47
<i>Inspector of Transport Security Act 2006</i>	ss 37(7); 61; 62; 63(1), (2), (3); 64(2), (3), (4), (5); 68; 69; 77(9)
<i>International Criminal Court Act 2002</i>	s 13
<i>Migration Act 1958</i>	ss 46A(5); 46B(5); 48B(4); 72(5); 91F(4); 91L(4); 91Q; 91Y; 195A(7); 197AG(2); 503A(1), (5)

<b>Other secrecy provisions</b>	
<b>Legislation</b>	<b>Provision</b>
<i>Military Rehabilitation and Compensation Act 2004</i>	s 409
<i>National Health and Medical Research Council Act 1992</i>	s 78(1)
<i>National Health Regulations 1954</i>	reg 32
<i>National Residue Survey Administration Act 1992</i>	s 11(1)
<i>National Workplace Relations Consultative Council Act 2002</i>	s 5
<i>Native Title Act 1993</i>	ss 24BF(2); 24CF(2); 24CI(3); 24DG(2); 24DJ(3); 31(4); 44B(4A); 44F(2); 86F(2A); 98A(2); 203BK(4)
<i>Occupational Health and Safety (Safety Standards) Regulations 1994</i>	regs 8.61; 9.68
<i>Offshore Petroleum Act 2006</i>	ss 422; 423; 425; 426; sch 5 cl 4
<i>Ombudsman Act 1976</i>	ss 19U; 35A; 35B; 35C
<i>Parliamentary Service Act 1999</i>	s 13(6)
<i>Patents Act 1990</i>	ss 56; 183
<i>Privacy (Private Sector) Regulations 2001</i>	sch 1 cl 4.6
<i>Public Service Act 1999</i>	s 13(6)
<i>Public Service Regulations 1999</i>	reg 2.1
<i>Research Involving Human Embryos Act 2002</i>	s 29(4)
<i>Social Security (Administration) Act 1999</i>	sch 3 cl 19

**Other secrecy provisions**

<b>Legislation</b>	<b>Provision</b>
<i>Telecommunications (Consumer Protection and Service Standards) Act 1999</i>	ss 22; 22A
<i>Telecommunications (Interception and Access) Act 1979</i>	s 202
<i>Therapeutic Goods Act 1989</i>	s 9C
<i>Trade Marks Act 1995</i>	s 258
<i>Trade Practices Act 1974</i>	ss 10.37; 10.88; 15AA; 44AAF; 89(5A); 95; 95AI; 95AZA; 95ZN; 155AAA
<i>Trade Practices Regulations 1974</i>	reg 7D
<i>Veterans' Entitlements Act 1986</i>	ss 34; 35H; 36L; 37L; 38L; 45Q; 57E; 79I; 93ZE; 116D; 118ZF; 118ZX; 137; 140; 196ZD
<i>Water Act 2007</i>	s 215
<i>Witness Protection Act 1994</i>	s 16
<i>Workplace Relations Act 1996</i>	ss 163C; 166T; 485; 702; 707; 712; 715; sch 1 cl 276

# Appendix 5. Extracts of Key Secrecy Provisions

---

## Contents

<i>Crimes Act 1914 (Cth)</i>	583
Section 70—Disclosure of information by Commonwealth officers	583
Section 79—Official secrets	584
Section 83—Unlawful soundings	587
<i>Criminal Code Act 1995 (Cth)</i>	588
Section 91.1—Espionage and similar activities	588
Section 91.2—Defence—information lawfully available	590
Dictionary—Definition of ‘Commonwealth public official’	590
<i>Intelligence Services Act 2001 (Cth)</i>	592
Section 39—Communication of certain information—ASIS	592
Section 39A—Communication of certain information—DIGO	593
Section 40—Communication of certain information—DSD	594
<i>Public Service Regulations 1999 (Cth)</i>	595
Regulation 2.1—Duty not to disclose information (Act s 13)	595

The following extracts include some of the principal provisions referred to in the text of this Issues Paper. Provisions referred to in passing only, or otherwise adequately set out in the text, are not included in this Appendix.

### ***Crimes Act 1914 (Cth)***

#### **Section 70—Disclosure of information by Commonwealth officers**

- (1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he or she is authorized to publish or communicate it, any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer, and which it is his or her duty not to disclose, shall be guilty of an offence.
  
- (2) A person who, having been a Commonwealth officer, publishes or communicates, without lawful authority or excuse (proof whereof shall lie upon him or her), any fact or document which came to his or her knowledge, or into his or her possession, by virtue of having been a Commonwealth officer, and which, at the time when he or she ceased to be a Commonwealth officer, it was his or her duty not to disclose, shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

**Section 79—Official secrets**

- (1) For the purposes of this section, a sketch, plan, photograph, model, cipher, note, document, or article is a prescribed sketch, plan, photograph, model, cipher, note, document or article in relation to a person, and information is prescribed information in relation to a person, if the person has it in his or her possession or control and:
- (a) it has been made or obtained in contravention of this Part or in contravention of section 91.1 of the *Criminal Code*;
  - (b) it has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he or she has made or obtained it owing to his or her position as a person:
    - (i) who is or has been a Commonwealth officer;
    - (ii) who holds or has held office under the Queen;
    - (iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth;
    - (iv) who is or has been employed by or under a person to whom a preceding subparagraph applies; or
    - (v) acting with the permission of a Minister;and, by reason of its nature or the circumstances under which it was entrusted to him or her or it was made or obtained by him or her or for any other reason, it is his or her duty to treat it as secret; or
  - (c) it relates to a prohibited place or anything in a prohibited place and:
    - (i) he or she knows; or
    - (ii) by reason of its nature or the circumstances under which it came into his or her possession or control or for any other reason, he or she ought to know;that it should not be communicated to a person not authorized to receive it.
- (2) If a person with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions:
- (a) communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, to a person, other than:
    - (i) a person to whom he or she is authorized to communicate it; or
    - (ii) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it;

or permits a person, other than a person referred to in subparagraph (i) or (ii), to have access to it;

- (b) retains a prescribed sketch, plan, photograph, model, cipher, note, document or article in his or her possession or control when he or she has no right to retain it or when it is contrary to his or her duty to retain it; or
- (c) fails to comply with a direction given by lawful authority with respect to the retention or disposal of a prescribed sketch, plan, photograph, model, cipher, note, document or article;

he or she shall be guilty of an indictable offence.

Penalty: Imprisonment for 7 years.

- (3) If a person communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, to a person, other than:

- (a) a person to whom he or she is authorized to communicate it; or
- (b) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it;

or permits a person, other than a person referred to in paragraph (a) or (b), to have access to it, he or she shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

- (4) If a person:

- (a) retains a prescribed sketch, plan, photograph, model, cipher, note, document or article in his or her possession or control when he or she has no right to retain it or when it is contrary to his or her duty to retain it;
- (b) fails to comply with a direction given by lawful authority with respect to the retention or disposal of a prescribed sketch, plan, photograph, model, cipher, note, document or article; or
- (c) fails to take reasonable care of a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, or to ensure that it is not communicated to a person not authorized to receive it or so conducts himself or herself as to endanger its safety;

he or she shall be guilty of an offence.

Penalty: Imprisonment for 6 months.

- (5) If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing or having reasonable ground to believe, at the time when he or she receives it, that it is communicated to him or her in contravention of section 91.1 of the *Criminal Code* or subsection (2) of this section, he or she shall be guilty of an indictable offence unless he or she proves that the communication was contrary to his or her desire.

Penalty: Imprisonment for 7 years.

- (6) If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing, or having reasonable ground to believe, at the time when he or she receives it, that it is communicated to him or her in contravention of subsection (3), he or she shall be guilty of an offence unless he or she proves that the communication was contrary to his or her desire.

Penalty: Imprisonment for 2 years.

- (7) On a prosecution under subsection (2) it is not necessary to show that the accused person was guilty of a particular act tending to show an intention to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions and, notwithstanding that such an act is not proved against him or her, he or she may be convicted if, from the circumstances of the case, from his or her conduct or from his or her known character as proved, it appears that his or her intention was to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions.

- (8) On a prosecution under this section, evidence is not admissible by virtue of subsection (7) if the magistrate exercising jurisdiction with respect to the examination and commitment for trial of the defendant, or the judge presiding at the trial, as the case may be, is of the opinion that that evidence, if admitted:

- (a) would not tend to show that the defendant intended to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions; or
- (b) would, having regard to all the circumstances of the case and notwithstanding subsection (9), prejudice the fair trial of the defendant.

- (9) If evidence referred to in subsection (8) is admitted at the trial, the judge shall direct the jury that the evidence may be taken into account by the jury only on the question whether the defendant intended to prejudice the security or defence

of the Commonwealth or a part of the Queen's dominions and must be disregarded by the jury in relation to any other question.

- (10) A person charged with an offence against subsection (2) may be found guilty of an offence against subsection (3) or (4) and a person charged with an offence against subsection (5) may be found guilty of an offence against subsection (6).

### **Section 83—Unlawful soundings**

- (1) Any person who in the Commonwealth or in any Territory:
- (a) takes any unlawful soundings;
  - (b) makes any record of any unlawful soundings;
  - (c) intentionally has in possession any record of unlawful soundings;
  - (d) communicates to any person outside the Commonwealth or any Territory any record of or information concerning unlawful soundings; or
  - (e) communicates to any other person any record of or information concerning unlawful soundings with intent that the record or information may be communicated to any person outside the Commonwealth or any Territory;

shall be guilty of an indictable offence.

Penalty: Imprisonment for 2 years.

- (2) For the purposes of this section all soundings taken in the territorial waters of the Commonwealth or any Territory shall be deemed to be unlawful unless they were made under the authority of the Queen, the Commonwealth Government, or a State Government, or the Government of a Territory, or were reasonably necessary for the navigation of the vessel from which they were taken or for any purpose in which the vessel from which they were taken was lawfully engaged.
- (3) In any prosecution under this section, proof that any soundings were not unlawfully taken shall lie upon the defendant.
- (4) Any figure or word or sign representing a figure (other than the printed figures appearing on any official or recognized map or chart) appearing on any map or sketch of any portion of the coast or territorial waters of Australia or of a Territory shall, in the absence of satisfactory proof to the contrary, be deemed to be a record of an unlawful sounding, but nothing in this subsection shall affect proof of unlawful soundings in any other manner.

- (5) All records of unlawful soundings including all maps or charts having thereon any record of unlawful soundings shall be forfeited to the Commonwealth.
- (6) A reference in this section to soundings shall be read as including a reference to a hydrographic survey and a reference to the taking of soundings shall be read as including a reference to the making of a hydrographic survey.

***Criminal Code Act 1995 (Cth)*****Section 91.1—Espionage and similar activities**

- (1) A person commits an offence if:
  - (a) the person communicates, or makes available:
    - (i) information concerning the Commonwealth's security or defence; or
    - (ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and
  - (b) the person does so intending to prejudice the Commonwealth's security or defence; and
  - (c) the person's act results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation.

Penalty: Imprisonment for 25 years.

- (2) A person commits an offence if:
  - (a) the person communicates, or makes available:
    - (i) information concerning the Commonwealth's security or defence; or
    - (ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and
  - (b) the person does so:
    - (i) without lawful authority; and
    - (ii) intending to give an advantage to another country's security or defence; and

- (c) the person's act results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation.

Penalty: Imprisonment for 25 years.

- (3) A person commits an offence if:

- (a) the person makes, obtains or copies a record (in any form) of:
- (i) information concerning the Commonwealth's security or defence; or
  - (ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and
- (b) the person does so:
- (i) intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation; and
  - (ii) intending to prejudice the Commonwealth's security or defence.

Penalty: Imprisonment for 25 years.

- (4) A person commits an offence if:

- (a) the person makes, obtains or copies a record (in any form) of:
- (i) information concerning the Commonwealth's security or defence; or
  - (ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and
- (b) the person does so:
- (i) without lawful authority; and
  - (ii) intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation; and
  - (iii) intending to give an advantage to another country's security or defence.

Penalty: Imprisonment for 25 years.

- (5) For the purposes of subparagraphs (3)(b)(i) and (4)(b)(ii), the person concerned does not need to have a particular country, foreign organisation or person in mind at the time when the person makes, obtains or copies the record.
- (6) A person charged with an offence under this section may only be remanded on bail by a judge of the Supreme Court of a State or Territory. This subsection has effect despite anything in section 93.1.

Note: Section 93.1 deals with how a prosecution is instituted.

- (7) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to offences under this section.

### **Section 91.2—Defence—information lawfully available**

- (1) It is a defence to a prosecution of an offence against subsection 91.1(1) or (2) that the information the person communicates or makes available is information that has already been communicated or made available to the public with the authority of the Commonwealth.
- (2) It is a defence to a prosecution of an offence against subsection 91.1(3) or (4) that the record of information the person makes, obtains or copies is a record of information that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matters in subsections (1) and (2). See subsection 13.3(3).

### **Dictionary—Definition of ‘Commonwealth public official’**

*Commonwealth public official* means:

- (a) the Governor-General; or
- (b) a person appointed to administer the Government of the Commonwealth under section 4 of the Constitution; or
- (c) a Minister; or
- (d) a Parliamentary Secretary; or
- (e) a member of either House of the Parliament; or
- (f) an individual who holds an appointment under section 67 of the Constitution; or

- (g) the Administrator, an Acting Administrator, or a Deputy Administrator, of the Northern Territory; or
- (h) the Administrator, an Acting Administrator, or a Deputy Administrator, of Norfolk Island; or
- (i) a Commonwealth judicial officer; or
- (j) an APS employee; or
- (k) an individual employed by the Commonwealth otherwise than under the *Public Service Act 1999*; or
- (l) a member of the Australian Defence Force; or
- (m) a member or special member of the Australian Federal Police; or
- (n) an individual who holds or performs the duties of an office established by or under a law of the Commonwealth, other than:
  - (i) the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*; or
  - (ii) the *Australian Capital Territory (Self-Government) Act 1988*; or
  - (iii) the *Corporations Act 2001*; or
  - (iv) the *Norfolk Island Act 1979*; or
  - (v) the *Northern Territory (Self-Government) Act 1978*; or
  - (vi) Part 2 of Chapter 2 of Schedule 1 to the *Workplace Relations Act 1996*; or
  - (vii) Schedule 10 to the *Workplace Relations Act 1996*; or
- (o) an officer or employee of a Commonwealth authority; or
- (p) an individual who is a contracted service provider for a Commonwealth contract; or
- (q) an individual who is an officer or employee of a contracted service provider for a Commonwealth contract and who provides services for the purposes (whether direct or indirect) of the Commonwealth contract; or
- (r) an individual who exercises powers, or performs functions, conferred on the person by or under a law of the Commonwealth, other than:

- (i) the *Corporations (Aboriginal and Torres Strait Islander) Act 2006*; or
  - (ii) the *Australian Capital Territory (Self-Government) Act 1988*; or
  - (iii) the *Corporations Act 2001*; or
  - (iv) the *Norfolk Island Act 1979*; or
  - (v) the *Northern Territory (Self-Government) Act 1978*; or
  - (vi) Part 2 of Chapter 2 of Schedule 1B to the *Workplace Relations Act 1996*; or
  - (vii) a provision specified in the regulations; or
- (s) an individual who exercises powers, or performs functions, conferred on the person under a law in force in the Territory of Christmas Island or the Territory of Cocos (Keeling) Islands (whether the law is a law of the Commonwealth or a law of the Territory concerned); or
- (t) the Registrar, or a Deputy Registrar, of Aboriginal and Torres Strait Islander Corporations.

### ***Intelligence Services Act 2001 (Cth)***

#### **Section 39—Communication of certain information—ASIS**

- (1) A person is guilty of an offence if:
- (a) the person communicates any information or matter that was prepared by or on behalf of ASIS in connection with its functions or relates to the performance by ASIS of its functions; and
  - (b) the information or matter has come to the knowledge or into the possession of the person by reason of:
    - (i) his or her being, or having been, a staff member or agent of ASIS; or
    - (ii) his or her having entered into any contract, agreement or arrangement with ASIS; or
    - (iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS; and
  - (c) the communication was not made:
    - (i) to the Director-General or a staff member by the person in the course of the person's duties as a staff member; or
    - (ii) to the Director-General or a staff member by the person in accordance with a contract, agreement or arrangement; or

- (iii) by the person in the course of the person's duties as a staff member or agent, within the limits of authority conferred on the person by the Director-General; or
- (iv) with the approval of the Director-General or of a staff member having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

- (2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

### **Section 39A—Communication of certain information—DIGO**

- (1) A person commits an offence if:

- (a) the person communicates any information or matter that was prepared by or on behalf of DIGO in connection with its functions or relates to the performance by DIGO of its functions; and
- (b) the information or matter has come to the knowledge or into the possession of the person by reason of:
  - (i) his or her being, or having been, a staff member of DIGO; or
  - (ii) his or her having entered into any contract, agreement or arrangement with DIGO; or
  - (iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DIGO; and
- (c) the communication was not made:
  - (i) to the Director of DIGO or a staff member by the person in the course of the person's duties as a staff member; or
  - (ii) to the Director of DIGO or a staff member by the person in accordance with a contract, agreement or arrangement; or
  - (iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director of DIGO; or
  - (iv) with the approval of the Director of DIGO or of a staff member having the authority of the Director of DIGO to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

- (2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

### **Section 40—Communication of certain information—DSD**

- (1) A person is guilty of an offence if:
- (a) the person communicates any information or matter that was prepared by or on behalf of DSD in connection with its functions or relates to the performance by DSD of its functions; and
  - (b) the information or matter has come to the knowledge or into the possession of the person by reason of:
    - (i) his or her being, or having been, a staff member of DSD; or
    - (ii) his or her having entered into any contract, agreement or arrangement with DSD; or
    - (iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DSD; and
  - (c) the communication was not made:
    - (i) to the Director of DSD or a staff member by the person in the course of the person's duties as a staff member; or
    - (ii) to the Director of DSD or a staff member by the person in accordance with a contract, agreement or arrangement; or
    - (iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director of DSD; or
    - (iv) with the approval of the Director of DSD or of a staff member having the authority of the Director of DSD to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

- (2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

***Public Service Regulations 1999 (Cth)*****Regulation 2.1—Duty not to disclose information (Act s 13)**

- (1) This regulation is made for subsection 13(13) of the Act.
- (2) This regulation does not affect other restrictions on the disclosure of information.
- (3) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.
- (4) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if the information:
  - (a) was, or is to be, communicated in confidence within the government; or
  - (b) was received in confidence by the government from a person or persons outside the government;whether or not the disclosure would found an action for breach of confidence.
- (5) Subregulations (3) and (4) do not prevent a disclosure of information by an APS employee if:
  - (a) the information is disclosed in the course of the APS employee's duties; or
  - (b) the information is disclosed in accordance with an authorisation given by an Agency Head; or
  - (c) the disclosure is otherwise authorised by law; or
  - (d) the information that is disclosed:
    - (i) is already in the public domain as the result of a disclosure of information that is lawful under these Regulations or another law; and
    - (ii) can be disclosed without disclosing, expressly or by implication, other information to which subregulation (3) or (4) applies.

- (6) Subregulations (3) and (4) do not limit the authority of an Agency Head to give lawful and reasonable directions in relation to the disclosure of information.

Note Under section 70 of the *Crimes Act 1914*, it is an offence for an APS employee to publish or communicate any fact or document which comes to the employee's knowledge, or into the employee's possession, by virtue of being a Commonwealth officer, and which it is the employee's duty not to disclose.