Australian Government

Australian Law Reform Commission

Secrecy Laws and Open Government in Australia

REPORT

REPORT 112
December 2009

This Report reflects the law as at 11 November 2009

ISBN- 978-0-9807194-0-6

Commission Reference: ALRC Report 112

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

Homepage: www.alrc.gov.au

Printed by Ligare

Australian Government

Australian Law Reform Commission

The Hon Robert McClelland MP
Attorney-General of Australia
Parliament House
Canberra ACT 2600

11 December 2009

Dear Attorney-General

Review of Secrecy Laws

On 5 August 2008, you issued terms of reference for the ALRC to undertake a comprehensive review of secrecy laws and related issues.

Those terms of reference were amended by your letter of 26 October 2009, to extend the reporting date to 11 December 2009, in order to facilitate the consideration of all submissions and consultations.

On behalf of the Members of the Commission involved in this Inquiry—including Justice Berna Collier and Justice Susan Kenny—and in accordance with the *Australian Law Reform Commission Act 1996* (Cth), I am pleased to present you with the final report in this reference, *Secrecy Laws and Open Government in Australia* (ALRC 112).

Yours sincerely

Professor Rosalind Croucher
Commissioner in charge
Acting President

Contents

Contents

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) (until 30 November 2009)
Professor Les McCrimmon (Commissioner) (until 30 November 2009)
Professor Rosalind Croucher (Commissioner in charge, and Acting President from 1 December 2009)
Justice Berna Collier (part-time Commissioner)
Justice Susan Kenny (part-time Commissioner)

Senior Legal Officers

Carolyn Adams
Bruce Alston (until July 2009)
Isabella Cosenza (until January 2009)

Legal Officers

Anna Dziedzic (from March 2009)
Lisa Eckstein
Althea Gibson (until January 2009)
Erin Mackay (until January 2009)

Consultant

Amie Grierson (March 2009)

Research Manager

Jonathan Dobinson

Librarian

Carolyn Kearney

Project Assistant

Tina O'Brien

Legal Interns

Michael Evry
Stephanie Fusco
Kelvin Liew
Isley Markman
Katherine McGree
Larisa Michalko
Tracy Nau
Naomi Oreb
Christina Ray
Michelle Salomon
Vasudha Sathanapally
Katie Schafer
Smriti Sriram
Yi-Shun Teoh
Michael Wells
Rebecca Zaman

Advisory Committee Members

Ms Lynelle Briggs, Australian Public Service Commissioner (until August 2009)
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
Ms Karin Fisher, Australian Public Service Commission (from August 2009)
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 Paterson, Law Faculty, Monash University
Mr Peter Timmins, Timmins Consulting
Ms Annette Willing, Australian Government Attorney-General's Department

List of Recommendations

4. Framework for Reform

Recommendation 4–1 Sections 70 and 79(3) of the *Crimes Act 1914* (Cth) should be repealed and replaced by new offences in the *Criminal Code* (Cth)—the 'general secrecy offence' and the 'subsequent disclosure offences'.

5. General Secrecy Offence: Harm to Public Interests

Recommendation 5–1 The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:

(a) damage the security, defence or international relations of the Commonwealth;

(b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;

(c) endanger the life or physical safety of any person; or

(d) prejudice the protection of public safety.

Recommendation 5–2 The terms 'security' and 'international relations' should be defined for the purposes of the general secrecy offence by reference to the relevant provisions of the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

6. General Secrecy Offence: Elements

Recommendation 6–1 The 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; or

(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.

Recommendation 6–2 The general secrecy offence should regulate the disclosure of Commonwealth information as defined in Recommendation 6–3.

Recommendation 6–3 The 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 Recommendation 6–1.

Recommendation 6–4 The general secrecy offence should require intention as the fault element attaching to the physical element consisting of disclosure.

Recommendation 6–5 The general secrecy offence should require that a Commonwealth officer knew, intended that, or was reckless as to whether, the disclosure of Commonwealth information would harm, or was reasonably likely to harm, one of the public interests set out in Recommendation 5–1.

Recommendation 6–6 There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) in breach of the general secrecy offence; and

(b) B knows, or is reckless as to whether, the information has been disclosed in breach of the general secrecy offence; and

(c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.

Recommendation 6–7 There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) on terms requiring it to be held in confidence;

(b) B knows, or is reckless as to whether, the information has been disclosed on terms requiring it to be held in confidence; and

(c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.

7. General Secrecy Offence: Exceptions and Penalties

Recommendation 7–1 The 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) in accordance with an authorisation given by an agency head or minister that the disclosure would, on balance, be in the public interest; or

(c) of information that is already in the public domain as the result of a lawful disclosure.

Recommendation 7–2 The subsequent disclosure offences should include an exception where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.

Recommendation 7–3 In developing public interest disclosure legislation the Australian Government should ensure that the legislation protects:

(a) individuals subject to the general secrecy offence;

(b) individuals who subsequently disclose Commonwealth information received by way of a protected public interest disclosure; and

(c) individuals subject to the subsequent disclosure offence for the unauthorised disclosure of information received from a Commonwealth officer on terms requiring it to be held in confidence.

Recommendation 7–4 The general secrecy offence should stipulate a maximum penalty of seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both.

Recommendation 7–5 The subsequent disclosure offences should stipulate maximum penalties of seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both.

Recommendation 7–6 The general secrecy offence and the subsequent disclosure offences 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 disclosure of the information.

8. The Role of Specific Secrecy Offences

Recommendation 8–1 Specific secrecy offences are only warranted where they are necessary and proportionate to the protection of essential public interests of sufficient importance to justify criminal sanctions.

Recommendation 8–2 Specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest, except where:

(a) the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit; or

(b) the harm is to the relationship of trust between individuals and the Australian Government integral to the regulatory functions of government.

Recommendation 8–3 Specific secrecy offences should differ in significant and justifiable ways from the recommended general secrecy offence.

9. Specific Secrecy Offences: Elements

Recommendation 9–1 Specific secrecy offences that apply to individuals other than Commonwealth officers should clearly identify the parties regulated by the offence.

Recommendation 9–2 Specific secrecy offences that apply to Commonwealth officers should also apply to former Commonwealth officers.

Recommendation 9–3 Specific secrecy offences should not extend to conduct other than the disclosure of information—such as making a record of, receiving or possessing information—unless such conduct would cause, or is likely or intended to cause, harm to an essential public interest.

Recommendation 9–4 Specific secrecy offences should generally require intention as the fault element for the physical element consisting of conduct. Strict liability should not attach to the conduct element of any specific secrecy offence.

Recommendation 9–5 Specific secrecy offences with an express harm requirement should generally require that a person knew, intended that, or was reckless as to whether, the conduct would cause harm to an essential public interest.

Recommendation 9–6 Specific secrecy offences without an express harm requirement should require that a person knew, or was reckless as to whether, the protected information fell within a particular category, and should not provide that strict liability applies to that circumstance.

Recommendation 9–7 Offences for the subsequent unauthorised disclosure of information should require that:

(a) the information has been disclosed in breach of a specific secrecy offence;

(b) the person knows, or is reckless as to whether, the information has been disclosed in breach of a specific secrecy offence; and

(c) the person knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—a specified essential public interest.

Recommendation 9–8 Maximum penalties in specific secrecy offences should reflect the seriousness of the potential harm caused by the unauthorised conduct and the fault elements that attach to the elements of the offence.

Recommendation 9–9 Specific secrecy offences should not generally prescribe:

(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 alternative 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 on indictment.

10. Authorised Disclosure Provisions

Recommendation 10–1 Where a specific secrecy offence is repealed or amended as a result of Recommendation 11–1, consideration should be given as to whether any provisions which codify authorised information handling should be retained.

Recommendation 10–2 Specific secrecy provisions that impose secrecy obligations on officers should generally include an exception for disclosures in the course of an officer's functions or duties.

Recommendation 10–3 Specific secrecy offences should not apply to the disclosure of information that is lawfully in the public domain.

Recommendation 10–4 Exceptions and defences in specific secrecy offences should be framed consistently with the principles set out in the *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*.

Recommendation 10–5 In developing public interest disclosure legislation the Australian Government should ensure that, where possible, the legislation protects individuals subject to specific secrecy offences.

11. Specific Secrecy Offences: Review and Guidance

Recommendation 11–1 Australian Government agencies should review specific secrecy offences to determine:

(a) whether a criminal offence is warranted;

(b) if so, whether the secrecy offence complies with the best practice principles set out in Recommendations 8–1 to 8–3, 9–1 to 9–9 and 10–1 to 10–4; and

(c) whether it would be appropriate to consolidate secrecy offences into:

(i) a single provision or part where multiple secrecy provisions exist in the same Act; or

(ii) one Act where secrecy offences exist in more than one Act for which the same Australian Government agency is responsible.

Recommendation 11–2 The Australian Government Attorney-General's Department should incorporate guidance on the principles contained in Recommendations 8–1 to 8–3, 9–1 to 9–9 and 10–1 to 10–4 in the *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, including:

(a) the circumstances in which the enactment of a specific secrecy offence will be justified; and

(b) the elements of specific secrecy offences, including the requirement that the disclosure cause harm to an essential public interest.

12. Administrative Obligations in the Australian Public Service

Recommendation 12–1 Regulation 2.1(3) of the *Public Service Regulations 1999* (Cth) should be amended to apply to information where the disclosure is reasonably likely to prejudice the effective working of government.

Recommendation 12–2 The Australian Public Service Commission should amend the *APS Values and Code of Conduct in Practice* to provide further guidance on what is meant by 'reasonably likely to prejudice the effective working of government' in reg 2.1 of the *Public Service Regulations 1999* (Cth), as revised in Recommendation 12–1. This should include:

(a) that prejudice may arise from the nature of the information disclosed, such as where the information would not be subject to release under the *Freedom of Information Act 1982* (Cth) or through some other means;

(b) that prejudice may arise from the circumstances in which the disclosure is made, such as where an Australian Public Service employee did not take reasonable steps to comply with the agency's information-handling policy or any lawful and reasonable direction concerning the disclosure of information; and

(c) the fact that a disclosure could, for example, result in embarrassment to the government is not sufficient to establish prejudice.

Recommendation 12–3 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.

Recommendation 12–4 The information-handling policies developed by Australian Government agencies in accordance with Recommendation 14–1 should set out the disciplinary penalties that may result from breach of secrecy obligations and an inclusive list of the factors that will be considered in determining a penalty.

13. Regulating Beyond the Australian Public Service

Recommendation 13–1 Australian Government agencies that employ persons other than under the *Public Service Act 1999* (Cth) should, to the extent that it is consistent with agency functions and structure:

(a) include the requirements in reg 2.1 of the *Public Service Regulations 1999* (Cth) in terms and conditions of employment; and

(b) adopt the safeguards under the *Public Service Act* for dealing with suspected breaches of reg 2.1.

Recommendation 13–2 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.

Recommendation 13–3 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 information or 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 is protected under Commonwealth public interest disclosure legislation.

Recommendation 13–4 Private sector organisations that perform services for or on behalf of the Australian Government under contract should ensure that all employees who have access to Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal and civil liability could result.

Recommendation 13–5 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) a right to terminate the appointment of a member in the event of a breach of the secrecy obligation.

Recommendation 13–6 The Australian Government should ensure that members of boards and committees who have access to Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal and civil liability could result.

14. Frameworks for Effective Information Handling

Recommendation 14–1 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;

(c) the circumstances in which the unauthorised handling of information could lead to disciplinary action; and

(d) the circumstances in which the unauthorised handling of information could lead to criminal prosecution.

Recommendation 14–2 Australian Government agencies should make their information-handling policies publicly available, save in certain exceptional cases where this would be unreasonable or impractical.

Recommendation 14–3 Australian Government agencies should review 'lawful and reasonable' secrecy directions issued to employees to ensure that these are consistent with the implied constitutional freedom of political communication.

Recommendation 14–4 Australian Government agencies that regularly share information with other agencies or bodies should enter into memorandums of understanding (MOUs) setting out the terms and conditions for the exchange of information. Australian Government agencies should make such MOUs publicly available save in certain exceptional cases where this would be unreasonable or impractical.

Recommendation 14–5 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.

15. A Culture of Effective Information Handling

Recommendation 15–1 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 need to share information in certain situations. Programs should also provide information about how employees can raise concerns and make public interest disclosures.

Recommendation 15–2 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.

Recommendation 15–3 The information-handling policies developed by Australian Government agencies in accordance with Recommendation 14–1 should set out how employees can raise concerns about their information-handling obligations.

Recommendation 15–4 The Information Commissioner should review and report to the Minister on the information-handling policies developed by Australian Government agencies in accordance with Recommendation 14–1 and any relevant employee directions.

16. Interactions with Other Laws

Recommendation 16–1 Section 38 of the *Freedom of Information Act 1982* (Cth) should be amended to include a definitive list of secrecy provisions that provide an exemption from the requirement to disclose documents under the Act.

Recommendation 16–2 When it is proposed to add a secrecy provision to the revised s 38 of the *Freedom of Information Act 1982* (Cth), the explanatory memorandum for the amending legislation should provide an assessment of the potential implications for open government, including:

(a) the breadth of the class of information to which the secrecy provision applies; and

(b) the likely significance for public scrutiny of government action.

Recommendation 16–3 Sections 91 and 92 of the *Freedom of Information Act 1982* (Cth) (FOI Act) should be amended to extend the indemnities from civil and criminal actions to authorised FOI officers who:

(a) disclose an exempt document under the FOI Act pursuant to a bona fide exercise of discretion not to claim the exemption; or

(b) disclose a document other than under the FOI Act provided that:

(i) the document would not have been exempt had it been requested under the FOI Act; or

(ii) the disclosure would have been a bona fide exercise of discretion not to claim an exemption had it been requested under the FOI Act.

Recommendation 16–4 The *Freedom of Information Act 1982* (Cth) should be amended to expressly override obligations of non-disclosure in other legislation.

Recommendation 16–5 Section 33(3) of the *Archives Act 1983* (Cth) should be repealed.

Recommendation 16–6 The *Archives Act 1983* (Cth) should be amended to provide that the public access provisions of the Act override any secrecy provisions that would otherwise apply.

Recommendation 16–7 The Australian Government should conduct a Privacy Impact Assessment for a proposed secrecy provision that would require or authorise information-handling practices that significantly detract from the standards set out in the *Privacy Act 1988* (Cth).

Executive Summary

Contents

Background

> Official secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not.[1]

Secrecy laws that impose obligations of confidentiality on individuals handling government information—and the prosecution of public servants for the unauthorised disclosure of such information—can sit uneasily with the Australian Government's commitment to open and accountable government. Secrecy laws have also drawn sustained criticism on the basis that they unreasonably interfere with the right to freedom of expression.

Against this background, 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 by providing appropriate access to information. The lack of consistency in secrecy provisions has been identified in a number of prior reviews, leading up to and prompting this Inquiry—including three prior reviews by the ALRC.[2] The ALRC was also asked to consider the increased need to share information within and between governments and with the private sector.

---

1 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [98]–[99].

2 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; Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 15–2.

The management of information can be conceived of as a spectrum, with openness of information and protection of information as opposite ends of that spectrum. Secrecy provisions are situated at different points in the spectrum—at times emphasising protection; at times facilitating information handling, sharing and disclosure.

The appropriate handling of information is integral to the effective functioning of government. Secrecy laws are one element in the broader information handling framework across government—including elements such as security classification systems, information-sharing regimes, and agency-specific information-handling policies. As part of the spectrum of information handling in the public sector, secrecy laws may serve a legitimate role in generating personal responsibility for the handling of Commonwealth information.

In the course of this Inquiry, the ALRC undertook a comprehensive mapping exercise to catalogue the secrecy provisions currently on the federal statute book. The ALRC identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences—a 'plethora' of provisions.[3] This mapping exercise provided a sound evidence base for the ALRC's analysis of secrecy provisions and the recommendations for reform in this Report.

A number of key issues emerged—including the catch-all nature of some of the provisions and an over-reliance on criminal sanctions. The ALRC also identified considerable inconsistency in the framing and elements of specific secrecy provisions, reflecting their introduction at different times, using different language and often with widely ranging penalties.

The challenge for the ALRC in this Inquiry was to identify the proper place for secrecy provisions in the context of a system of open and accountable government—consistent with Australia's obligations under international law, in particular the right to freedom of expression.

In addition, the ALRC considers that a regime enabling robust public interest disclosure—or whistleblower protection—is an essential element in an effective system of open government and a necessary complement to secrecy laws. In this regard, the ALRC reaffirms its recommendations made in previous reports that the Australian Government should legislate to introduce a comprehensive public interest disclosure legislation covering all Australian Government agencies.[4]

---

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

4 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 3–1; Australian Law Reform Commission, *Integrity: But Not by Trust Alone: AFP & NCA Complaints and Disciplinary Systems*, ALRC 82 (1996), Rec 117.

Focus of the recommendations

In this Report, the ALRC recommends a new and principled framework striking a fair balance between the public interest in open and accountable government and adequate protection for Commonwealth information that should legitimately be kept confidential.

The principles underpinning the ALRC's recommendations are that:

- administrative and disciplinary frameworks play the central role in ensuring that government information is handled appropriately, and that every person in the information chain understands their responsibilities in respect of that information;

- criminal sanctions should only be imposed where they are warranted—when the disclosure of government information is likely to cause harm to essential public interests—and where this is not the case, the unauthorised disclosure of information is more appropriately dealt with by the imposition of administrative penalties or the pursuit of contractual remedies;

- there is a continuing role for properly framed secrecy offences—both general and specific—in protecting Commonwealth information, provided that they are clear and consistent, and directed at protecting essential public interests.

In this Report, the ALRC considers three broad areas for reform. First, the ALRC recommends the repeal of the wide catch-all provisions currently in the *Crimes Act 1914* (Cth), and the introduction of a new general secrecy offence, limited to disclosures that harm essential public interests. Secondly, the ALRC considers the wide variety of other specific secrecy offences and recommends best practice principles to guide the review, repeal and amendment of these provisions. Thirdly, the ALRC considers the administrative frameworks governing those that handle government information and makes a range of recommendations to improve the management of government information within those frameworks.

A new general offence

The ALRC's key recommendation for reform is that the sanctions of the criminal law—in publicly punishing, deterring, and denouncing offending behaviour—should be reserved for behaviour that harms, is reasonably likely to harm or intended to harm essential public interests. The new general secrecy offence is limited to unauthorised disclosures that are likely to:

- damage the security, defence or international relations of the Commonwealth;

- prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;

- endanger the life or physical safety of any person; or
- prejudice the protection of public safety.

In formulating a provision to target the protection of essential public interests, the ALRC was drawn to the idea that the general secrecy offence should complement the *Freedom of Information Act 1982* (Cth) (FOI Act). 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 identifying information which, if disclosed, has the potential to prejudice the effective working of government.[5] The ALRC has adopted the approach that a subset of the public interests identified in the FOI Act exemptions should inform the development of the public interests to be protected by the general secrecy offence.

The new offence, to be included in the *Criminal Code*, is intended to replace s 70 of the *Crimes Act*, and to apply to all Commonwealth information and all present and former Commonwealth officers.

The ALRC also recommends two offences for the subsequent disclosure of Commonwealth information by third parties, where the information was initially disclosed to that person in breach of the general secrecy offence or on terms requiring it to be held in confidence.

The ALRC recommends that there should be exceptions in the general secrecy offence for disclosure in the course of an officer's functions or duties; disclosure with the authority of an agency head or minister; and disclosure of information that is already lawfully in the public domain. Protection from criminal liability under secrecy offences may also arise as a result of whistleblower legislation.

Specific secrecy offences

The ALRC considers that the new general secrecy offence should not be the only criminal provision regulating the unauthorised disclosure of government information. There is still a need for specific secrecy offences tailored to the needs of particular agencies or to the protection of certain kinds of information. In the interests of consistency and simplification, the ALRC recommends a set of principles to guide the creation of new offences and the review of existing offences.

The key principle is that specific secrecy offences should only be enacted where necessary to protect a public interest of sufficient importance to justify the imposition of a criminal sanction. As a general rule, the ALRC considers that the best way to ensure this is to include an express requirement that the unauthorised disclosure of

5 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009.

information caused, or was likely or intended to cause, harm to a specified public interest.

The ALRC recognises, however, that, in very limited circumstances, this may not always be the most effective way to address the harm caused by the disclosure of some kinds of information. For example, specific secrecy offences prohibiting the disclosure of information obtained or generated by intelligence agencies—without the need to prove harm in every case—are justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies.

Further, in very limited cases, and where the category of information protected is narrowly defined, regulatory agencies—such as taxation and social security, and corporate regulators—may also be able to justify specific secrecy offences that do not include an express harm requirement. This is because the public interest harmed by the unauthorised disclosure of information held by such agencies—that is, harm to the relationship of trust between the government and individuals that is integral to effective regulatory systems and the provision of government services—is not concrete enough to prove beyond reasonable doubt in a criminal prosecution.

The ALRC has also developed other best practice principles in relation to specific secrecy offences, including that such offences should:

- differ in significant and justifiable ways from the recommended general secrecy offence;
- not extend to conduct other than the disclosure of information—such as making a record of, receiving, or possessing information—unless such conduct would cause, or is likely or intended to cause, harm to an essential public interest; and
- specify penalties that reflect the seriousness of the potential harm caused by the unauthorised conduct and the criminal culpability of the offender.

While the primary focus of secrecy offences is to prohibit the disclosure of information, many secrecy provisions also include exceptions that set out the circumstances in which the disclosure of information is permitted. Such provisions often reflect the need for the government to share information. The ALRC also makes recommendations to ensure that specific secrecy offences are framed to facilitate appropriate information sharing, and are responsive to whole of government needs.

Administrative duties, practices and procedures

In the final part of the Report, the ALRC focuses upon the administrative secrecy framework in the Australian Government. The ALRC considers that secrecy provisions that impose administrative penalties on public sector employees have a central role to play—particularly where disclosure is inadvertent, there is no intention to cause harm,

or where any potential harm caused by the disclosure is relatively minor. Administrative penalties allow misconduct to be addressed in the employment context, reserving criminal sanctions only for those unauthorised disclosures that warrant the very serious consequences of criminal charge and conviction.

The principal administrative secrecy provision in the Australian Government is reg 2.1 of the *Public Service Regulations 1999* (Cth), which imposes a duty on all Australian Public Service (APS) employees not to disclose information where it is 'reasonably foreseeable' that the disclosure 'could be prejudicial to the effective working of government'. The ALRC recommends that the scope of conduct regulated by reg 2.1 should be narrowed. That is, it should only apply to disclosures that are 'reasonably likely' to result in such prejudice. This reform recognises the importance of promoting information sharing in appropriate circumstances. The ALRC further recommends that equivalent conduct standards should apply to most Commonwealth employees other than APS employees—such as employees of statutory authorities and ministerial staff.

Secrecy provisions do not operate in a vacuum. Administrative practices and procedures play a key role in influencing the circumstances in which an individual discloses government information. The ALRC makes a number of recommendations to promote an effective information-handling culture within Australian Government agencies. Importantly, the ALRC recommends that every Australian Government agency should develop and publish information-handling policies and guidelines to clarify the application of secrecy laws to their information holdings. Other strategies canvassed by the ALRC to promote effective information handling include the development of memorandums of understanding between agencies that regularly share information and ongoing training and development for all employees on information-handling obligations relevant to their position.

Finally, the ALRC recognises the importance of independent oversight of the manner in which Australian Government agencies discharge their information-handling responsibilities. To this end, the ALRC recommends a role for the proposed new Office of the Information Commissioner.

1. Introduction to the Inquiry

Contents

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 are set out at the front of this Report.

1.2 In the course of this Inquiry the ALRC has identified 506 secrecy provisions in Commonwealth legislation, including 358 criminal secrecy offences. These have been introduced at different times, using different language and often with widely ranging penalties. The ALRC has considered whether these secrecy provisions are comprehensive, consistent and workable in the context of the need for openness and accountability in the Australian Government. In particular, the ALRC has identified the need to reform of the general secrecy offences in ss 70 and 79(3) of the *Crimes Act 1914* (Cth).

1.3 The ALRC has also taken into account the need to share information within the Australian Government and more broadly. This is a particular focus of the ALRC's consideration of the ongoing need for specific secrecy provisions, and the development of information-handling policies and guidelines for people who handle Commonwealth information.

1.4 The ALRC's own legislation sets out certain parameters that affect policymaking and the formulation of recommendations. Section 24(1) of the *Australian Law Reform Commission Act 1996* (Cth) requires the ALRC, in performing its functions, to ensure that the laws, proposals and recommendations it reviews or considers:

> (a) do not trespass unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative, rather than judicial, decisions; and
>
> (b) are, as far as practicable, consistent with the International Covenant on Civil and Political Rights.

1.5 The ALRC is also required to have regard to all of Australia's international obligations that are relevant to the matter which is the subject of an inquiry.[1]

1.6 This Inquiry coincides with increased public attention on protections for 'whistleblowers' making disclosures in the public interest. In February 2009, the House of Representatives Standing Committee on Legal and Constitutional Affairs released its report, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector*. The Standing Committee recommended that a Public Interest Disclosure Bill be introduced to Parliament as a matter of priority.[2] 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.[3]

Previous calls for a review of secrecy provisions

1.7 The consistency and workability of Commonwealth secrecy provisions has been considered in a number of prior reviews, leading up to and prompting this Inquiry.

1.8 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 the general secrecy offence in s 70 of the *Crimes Act*, as it was 'implausible to enact a presumption of openness while

---

1 *Australian Law Reform Commission Act 1996* (Cth) s 24(2).

2 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.

3 Ibid, ix.

leaving untouched provisions like section 70 that provide the legal foundation for the system of discretionary secrecy that presently exists'.[4]

1.9 In 1983, the Human Rights Commission reviewed the *Crimes Act* and found that s 70 could operate in a manner inconsistent with the freedom of expression contained in art 19 of the *International Covenant on Civil and Political Rights*.[5]

1.10 In 1991, a committee chaired by Sir Harry Gibbs undertook a review of Commonwealth criminal law, including secrecy offences.[6] 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.[7]

1.11 In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs considered the operation of ss 70 and 79 of the *Crimes Act* and noted the longstanding calls for reform.[8] The Committee identified a number of problems with the sections, including a lack of precision in the drafting.[9] It also noted the lack of consistency in drafting and penalties across the secrecy provisions in other Commonwealth statutes.[10] The Committee recommended that existing secrecy provisions should be rationalised and consolidated into a general offence within the *Crimes Act*.[11]

1.12 The ALRC itself has commented on secrecy laws in three prior reviews. First, in the review of freedom of information laws in 1995, the ALRC and the Administrative Review Council recommended that a thorough review of all Commonwealth secrecy provisions be conducted to ensure that such provisions did not prevent the disclosure of information that was not exempt under the FOI Act.[12]

---

4 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), [21.24].

5 Human Rights Commission, *Review of the Crimes Act 1914 and Other Crimes Legislation of the Commonwealth* (1983). The relationship between freedom of expression and secrecy provisions is considered in Ch 2.

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

7 Ibid, 315.

8 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.

9 Ibid, 91–92.

10 Ibid, 95.

11 Ibid, 118.

12 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.

1.13 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* [*1999* (Cth)]—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.[13]

1.14 Finally, 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* [*1988* (Cth)].[14]

Matters outside this Inquiry

1.15 In reviewing Commonwealth secrecy laws, the Terms of Reference ask the ALRC to consider 'relevant laws and practices relating to the protection of Commonwealth information'. The protection of Commonwealth information can encompass matters as varied as how files and documents are physically protected; whether classification processes are appropriate and effective; and the extent to which Commonwealth officers can be compelled to produce Commonwealth information in the course of investigations or in legal proceedings.

1.16 The focus of this Inquiry is on statutory provisions concerning the secrecy and confidentiality obligations of individual Commonwealth officers (or other people nominated in legislation) in relation to Commonwealth information. Review of the government's larger information security and management systems is outside the scope of this Inquiry.

1.17 In ALRC 98, the ALRC considered the protection of classified and security sensitive information in the context of court and tribunal proceedings.[15] 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).

1.18 The extent to which Commonwealth officers can be compelled to provide information in the course of investigations or legal proceedings is not a focus of this Inquiry. The ALRC's approach in this Inquiry is informed by the emphasis in the

---

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

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

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.

Timeframe

1.19 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. The Terms of Reference initially stipulated a reporting date of 31 October 2009. In order to ensure that the views of key stakeholders could be considered fully, the ALRC requested, and the Attorney-General granted, an extension until 11 December 2009.[16]

Process of reform

Mapping secrecy laws

1.20 An integral component of the background research undertaken by the ALRC for this Inquiry was a 'mapping exercise' to identify and analyse the multitude of secrecy provisions in Commonwealth legislation. The 506 secrecy provisions identified by the ALRC are scattered throughout 176 pieces of primary and subordinate legislation administrative responsibility for which is spread across 19 departments of state.[17] Approximately 70% of the statutory secrecy provisions identified expressly impose criminal penalties.[18]

1.21 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 recommendations for reform. Figures drawn from the data are expressed throughout this Report 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.

Advisory Committee

1.22 A key aspect of the ALRC's reform process is to establish an expert Advisory Committee or 'reference group' to assist with the development of its inquiries. In this Inquiry, the Advisory Committee included a federal court judge, senior officers of Australian Government agencies, academics, senior lawyers, and an FOI consultant. [19]

1.23 The Advisory Committee has particular value in helping the ALRC to identify the key issues and determine priorities as well as providing quality assurance in the research, writing and consultation processes. The Advisory Committee also assists with the development of proposals and recommendations for reform. Ultimate responsibility

16 Attorney-General the Hon Robert McClelland MP, Letter to the ALRC, 16 October 2009.
17 These provisions are listed in a table in Appendix 4.
18 These provisions are listed in the first section of the table in Appendix 4.
19 A list of Advisory Committee members can be found in the List of Participants at the front of this Report.

for the Report and recommendations, however, remains with the Commissioners of the ALRC.

1.24 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 the Discussion Paper. A third meeting was held on 24 September 2009 to obtain input on options for reform.

Community consultation and participation

1.25 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'. One of the most important features of ALRC inquiries is the commitment to widespread community consultation.[20] 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.

Consultation meetings

1.26 During the course of this Inquiry the ALRC conducted 35 meetings with a number of Australian Government agencies, academics, judges and members of the legal profession. The consultations were designed to capture the views of a wide cross-section of interested stakeholders. A full list of agencies, organisations and individuals consulted is set out in Appendix 2.

Consultation documents

1.27 Two community consultation documents—an Issues Paper and a Discussion Paper[21]—were produced before proceeding to this final Report with recommendations for reform. In addition, 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, written in plain language and providing ready access to information about the Inquiry.

Submissions

1.28 The ALRC received 46 submissions in response to the Issues Paper, *Review of Secrecy Laws* (IP 34) and 38 submissions in response to the Discussion Paper, *Review of Secrecy Laws* (DP 74). A list of submissions is set out in Appendix 1. A number of individuals, groups and federal bodies made submissions to both IP 34 and DP 74. The ALRC acknowledges the considerable amount of work in preparing submissions and thanks all individuals and organisations who made submissions to this Inquiry.

---

20 B Opeskin, 'Measuring Success' in B Opeskin and D Weisbrot (eds), *The Promise of Law Reform* (2005), 202.

21 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008); Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009).

Online forum and national phone-in

1.29 In this Inquiry the ALRC utilised two additional strategies for consultation—an online forum and a national phone-in.

1.30 The national secrecy phone-in was conducted on 11 and 12 February 2009. The ALRC received 34 calls expressing concerns about matters such as: inappropriate revelations of personal information or perceived breaches of privacy; difficulties in gaining access to personal information, for example, for the purpose of family reunion; problems with security classifications and obtaining security clearances; cultures of secrecy in agencies; the need for whistleblower protection; difficulties in the sharing of information amongst agencies; and the draconian nature of s 70 of the *Crimes Act*.

1.31 To facilitate public communication in relation to the Inquiry, the ALRC also initiated a 'Talking Secrecy' online forum.[22] After moderation, the ALRC posted 12 contributions to the online forum. Comments included matters about agency culture; the security classification system; 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.

Overview of this Report

1.32 This Report contains 61 recommendations for reform. The focus of the recommendations is to provide a principled basis for a revised general secrecy offence, complemented by criteria for reforming specific secrecy provisions and revised administrative procedures and provisions aimed at fostering effective information handling in the public sector.

1.33 In accordance with its general policy, the ALRC has not produced draft legislation—for example, a draft general secrecy offence. 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. Where relevant, final recommendations specify the nature of any recommended legislative change.

Definitions

1.34 Several terms are used throughout this Inquiry. Some definitions are set out below.

---

22 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [1.92]–[1.93].

Secrecy provision

1.35 There is no established definition of the term 'secrecy law' or 'secrecy provision'. 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 on individuals or entities in relation to Commonwealth information.

1.36 Secrecy provisions normally apply to the disclosure of information. They may, however, cover a chain of conduct that leads to possible disclosure—such as soliciting, obtaining, copying, using and retaining information.

1.37 Provisions that have not been included in the concept of 'secrecy law' include those that:

- prohibit the misuse of information for personal gain—as the principal concern of such provisions is fraud, not the protection of the confidentiality of the information;[23]
- concern the storage, modification or destruction of information; or
- permit the disclosure of information in certain circumstances.

General and specific secrecy offences

1.38 The ALRC's consideration of criminal secrecy offences is divided into general and specific secrecy offences.

1.39 A *general* secrecy offence is intended to serve as an umbrella offence applying to the unauthorised disclosure of Commonwealth information by all current and former Commonwealth officers.

1.40 *Specific* secrecy provisions apply to particular agencies or individuals or protect particular kinds of information. Where such provisions create a criminal offence, the ALRC describes them as 'specific secrecy offences'.

Commonwealth information

1.41 'Commonwealth information' (also referred to as 'government' or 'official' information) is information developed, received or collected by or on behalf of the

---

23 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.

Commonwealth government. It includes information the Commonwealth receives from individuals (such as personal information provided to an agency like Centrelink), information developed in-house (for example, intelligence reports) and information generated by foreign governments that is shared with the Commonwealth government.

Essential public interests

1.42 In this Inquiry the ALRC focuses upon identifying those public interests that are sufficiently important to warrant protection through criminal secrecy offences. These are referred to as 'essential public interests'.

Whistleblowing

1.43 The ALRC has adopted the definition of 'public interest disclosure', or 'whistleblowing', set out in the text *Public Interest Disclosure Legislation in Australia*—that 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'.[24]

Chapter structure

1.44 This Report is divided into 16 chapters, falling into five broad areas:

- conceptual framework;
- a general criminal secrecy offence;
- specific secrecy offences;
- administrative duties, practices and procedures; and
- interactions with other laws.

Conceptual framework

1.45 The first four chapters provide the conceptual framework for secrecy laws, and an overview of the confidentiality and secrecy obligations imposed by common law and statute. This section also puts forward a framework for reform, including the idea that secrecy provisions should only be put in place to protect information that genuinely requires protection and where unauthorised disclosure has the potential to harm identified essential public interests.

1.46 Chapter 2 provides the broad conceptual framework for the Inquiry and the interaction and tension between ideas of secrecy and accountability of government. The chapter begins with a brief historical overview of the shift from secrecy towards

---

24 A Brown, *Public Interest Disclosure Legislation in Australia* (2006), xxi.

open government, followed by a review of current trends in open government. The chapter then considers the right of freedom of expression under the *International Covenant on Civil and Political Rights*,[25] concluding with a discussion of balancing ideas of secrecy, freedom of expression and open government.

1.47 Chapter 3 contains an overview of the laws that currently govern the use and disclosure of Commonwealth information by individuals within and beyond the Australian Government. It describes the equitable duty of confidence and common law duties of loyalty and fidelity in relation to the use and disclosure of government information. The chapter then examines the elements of specific secrecy provisions contained in Commonwealth legislation, and discusses the general secrecy offences set out in ss 70 and 79(3) of the *Crimes Act*.

1.48 Chapter 4 considers whether general law obligations—such as the equitable duty of confidence and the common law duty of loyalty and fidelity—provide sufficient protection in the public sector context. The ALRC concludes that, in addition, it is necessary and desirable to have in place statutory provisions that impose obligations on Commonwealth officers and others who handle Commonwealth information. The chapter also examines the potential role of administrative, civil and criminal statutory provisions in regulating the disclosure of Commonwealth information.

1.49 The ALRC's key recommendation for reform in the criminal context is that, in most cases, 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 an essential public interest, the ALRC has formed the 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.

A new general secrecy offence

1.50 Chapters 5 to 7 consider in detail the way the recommended new general secrecy offence should be framed, including which public interests should be expressly protected by the offence. In Chapter 5, the ALRC takes as its starting point the public interests protected by the various exemptions under the FOI Act. These exemptions are indicative of the situations in which the disclosure of Commonwealth information has the potential to harm the public interest. The ALRC examines each of the FOI Act exemptions and recommends which of these require the protection of the criminal law under the general secrecy offence.

1.51 Chapter 6 considers some of the other elements of the general secrecy offence, including whose conduct, and what kind of conduct, should be regulated. The ALRC

---

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

recommends two offences for the subsequent disclosure of Commonwealth information by third parties, where the information was initially disclosed to that person in breach of the general secrecy offence or on terms requiring it to be held in confidence.

1.52 Chapter 7 considers which exceptions and defences should be available under the recommended general secrecy offence and subsequent disclosure offences and the penalties that should apply for breach. The ALRC recommends that there should be exceptions in the general secrecy offence for disclosure in the course of an officer's functions or duties; disclosure with the authority of an agency head or minister; and disclosure of information that is already lawfully in the public domain. Protection from criminal liability under secrecy offences may also arise as a result of public interest disclosure (or 'whistleblower') legislation. The chapter considers the interaction of the recommended offences with public interest disclosure legislation as proposed by the House of Representatives Standing Committee on Legal and Constitutional Affairs.

Specific secrecy offences

1.53 Chapters 8 to 11 review specific secrecy offences—that is, secrecy offences other than ss 70 and 79(3) of the *Crimes Act*. These chapters consider the circumstances in which specific secrecy offences are warranted, and how such offences should be framed.

1.54 In Chapter 8, the ALRC recommends that specific secrecy offences are only warranted where they are necessary and proportionate to protect essential public interests. The chapter compares two ways of confining secrecy offences to conduct that causes harm to essential public interests—the inclusion of an express requirement of harm and the protection of certain categories of information in which the harm of disclosure may be implicit or not amenable to inclusion as an element of a criminal offence. The chapter considers three categories of information in detail: information obtained or generated by intelligence agencies; information obtained or generated by law enforcement agencies; and personal and commercial information.

1.55 In Chapter 9, the ALRC makes recommendations in relation to other elements of specific secrecy offences, including whose conduct and what conduct should be regulated by specific secrecy offences, as well as appropriate fault elements and penalties for contravention of secrecy offences. The chapter also considers specific subsequent disclosure offences.

1.56 Chapter 10 discusses the way in which secrecy offences may both prohibit the disclosure of information, and also set out circumstances in which the disclosure of information is permitted. The chapter considers when it may be appropriate to include authorised disclosure provisions in legislation to enable Commonwealth information to be shared in appropriate circumstances and the form that those provisions should take. In addition, the ALRC considers how authorised disclosure provisions in specific

legislation can provide content to the exceptions and defences recommended to be included in the general secrecy offence.

1.57 Chapter 11 discusses how the ALRC's recommendations in Chapters 8 to 10 can be applied to specific secrecy offences currently on the Commonwealth statute book and to the creation of new secrecy offences in the future. The ALRC considers how current specific secrecy offences might be reviewed and recommends the development of policy guidance to assist in drafting secrecy offences.

Administrative duties, practices and procedures

1.58 In contrast to the focus on criminal secrecy offences in preceding chapters, the four chapters in this group discuss the administrative secrecy framework in the Australian Government. The cornerstone of this framework is the secrecy provision set out in reg 2.1 of the *Public Service Regulations*, which applies to all Australian Public Service (APS) employees. Chapter 12 considers in detail this regulation and associated provisions of the *Public Service Act 1999* (Cth). In particular, the chapter makes recommendations for narrowing the scope of conduct regulated by reg 2.1 to promote information sharing in appropriate circumstances.

1.59 Regulation 2.1 and associated provisions only apply to APS employees. In Chapter 13, the ALRC recommends 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 statutory 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.

1.60 Chapters 14 and 15 discuss 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.

Interaction with other information-handling laws

1.61 Chapter 16 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). The ALRC makes recommendations to promote public comment and deliberation before enactment of a secrecy provision that would detract from the disclosure requirements under the FOI Act or the information-handling standards set out in the *Privacy Act*. The chapter also considers the interaction between secrecy laws and parliamentary privilege.

Stop press—legislation recently introduced into Parliament

1.62 The law in this Report is current to 11 November 2009. Following this date, three significant bills were introduced into Parliament—two proposed amendments to the FOI Act and one concerning taxation secrecy provisions.

1.63 The Freedom of Information Amendment (Reform) Bill 2009 (Cth) and the Information Commissioner Bill 2009 (Cth) were introduced in Parliament on 26 November 2009. The Bills closely reflect exposure drafts, released for public comment in March 2009, which have been quoted extensively by the ALRC in this Report.[26] As noted in Chapters 2 and 16, these reforms aim to promote a pro-disclosure culture across the Australian Government including the rationalisation of exemptions to the right of access, mandating the proactive publication of certain information, and establishing the Office of the Information Commissioner as an independent monitor in relation to FOI. There appear to be few significant changes from the Exposure Draft Bills. The most notable difference for the purpose of this Inquiry is the removal of the proposed public interest test for the exemption for trade secrets or other information of commercial value that would be destroyed or diminished by disclosure.[27]

1.64 On 30 November 2009, the Senate referred the Freedom of Information (Reform) Bill and Information Commissioner Bill to the Senate Finance and Public Administration Committee for inquiry and report.[28] Issues for consideration include:

- whether the measures in the Bills will ensure that the right of access is as comprehensive as it can be;
- whether the improvements to the process for requesting access are efficient and could be further improved;
- whether the measures will assist in the creation of a pro-disclosure culture in the Australian Government and what further measures may be appropriate; and
- assessment of the functions, powers and resources of the Information Commissioner.

1.65 On 19 November 2009, the Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 was introduced into the House of Representatives. The Bill proposes to consolidate the secrecy and disclosure provisions that are currently

---

26 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth); Exposure Draft, Information Commissioner Bill 2009 (Cth).

27 Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2 inserting new s 47. Other information about business affairs will continue to be subject to a public interest test: ibid sch 3 pt 2 inserting new s 47G.

28 The Senate Committee is due to report on 16 March 2010.

scattered across 18 different pieces of taxation legislation into a single comprehensive framework within the *Taxation Administration Act 1953* (Cth).

1.66 Prior to the introduction of this Bill, the Treasury released a *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* which canvassed issues in relation to the consistency and application of secrecy and disclosure provisions in Australia's taxation laws.[29] 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 of this Bill and accompanying Explanatory Material.[30] The ALRC has referred to the Draft Bill and Explanatory Material throughout this Report. While there have been some changes in the form of some provisions, there does not appear to be a significant difference between the content of the Exposure Draft Bill and the Bill introduced into Parliament.

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

30 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth); Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth).

2. Secrecy in the Context of Open Government

Contents

Introduction

2.1 In this Inquiry the ALRC has been asked to have regard to the importance of balancing the public interest in an open and accountable system of government with the need to protect Commonwealth information. The challenge then is to identify the proper place for secrecy provisions in the context of open government.

2.2 The concept of secrecy as a mechanism for protecting government information, on the one hand, and the commitment to openness of government, on the other, reflect certain historical understandings of the relationship between a government, citizens, officials and information. In setting the scene for a consideration of the role and function of secrecy provisions in Commonwealth laws today, this chapter will explore some of the key ideas and developments in the conceptual landscape.

2.3 The chapter begins with a brief historical overview of the shift from secrecy towards open government followed by a review of current trends in open government. The chapter then considers the right of freedom of expression under the *International*

Covenant on Civil and Political Rights (ICCPR),[1] concluding with a discussion of balancing concepts of secrecy, freedom of expression and open government.

From secrecy to open government

Secrecy and government

2.4 The secrecy of government information has a long history. As Professor Enid Campbell has explained, the notion that the activities of government should be secret goes back to a period when monarchs were motivated 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.[2] Two principal rationales for secrecy in the modern context are the Westminster system of government and the need to protect national security.

2.5 The Westminster system was premised on secrecy. As summarised by the Independent Review Panel examining the *Freedom of Information Act 1992* (Qld):

> 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.[3]

2.6 In this way, the conventions of the Westminster system were seen to demand official secrecy. For example, the doctrine of collective ministerial responsibility was said to depend to a large extent on the secrecy of Cabinet deliberations and documents. Further, the confidential provision of advice to ministers by public servants is linked to the principle that the government of the day is served by a professional and politically neutral public service carrying out the instructions of the elected government.[4]

2.7 For most of Australia's history, 'official secrecy has been the legislatively enforced norm'.[5] The first Australian secrecy provision, introduced in the colony of Victoria in 1867, 'set the pattern for the various public services of Australia', requiring that:

---

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

2 E Campbell, 'Public Access to Government Documents' (1976) 41 *Australian Law Journal* 73, 77.

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

4 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.

5 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 90.

> 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.[6]

2.8 The first Commonwealth secrecy provisions were passed during the initial session of the Australian Parliament in 1901.[7] Their primary focus was the protection of national security information.[8]

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'.[9] In 1960, amendments were made to s 70 of the *Crimes Act 1914* (Cth),[10] inspired in part by the anti-communist climate of the Cold War.[11] The amendment, which extended the reach of s 70 to former Commonwealth officers, was 'just one of many secrecy provisions inserted or strengthened in legislation after the war'.[12]

Secrecy and the expanding reach of government

2.10 The increase in the size and role of government in the period following World War II, combined with technological advances that increased the ability of governments to deal with large amounts of information, has had a significant impact on the relationship between citizens and government.[13] Information, as Greg Terrill has remarked, now 'underpins almost all of government activity'; and it is both an 'object in its own right' as well as 'a dimension of all government activity'.[14]

2.11 The increased reach of government was matched by a growth in secrecy provisions. John McGinness commented that the increase in secrecy provisions was 'a reflection of the increase in personal and commercially sensitive information collected by the government'.[15] In addition, the *Privacy Act 1988* (Cth) was enacted to ensure that the government appropriately handled and protected personal information. Both reflected the impetus to protect certain information in the hands of government.

---

6 Ibid. The provision was found in reg 20 of the 1867 Regulations for the *Civil Service Act 1862* (Vic): 9.

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

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

9 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 41. Terrill notes that 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'. The Cold War continued effectively until the collapse of the Soviet Union in 1991.

10 Section 70 of the *Crimes Act 1914* (Cth) is set out in Appendix 5.

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

12 Ibid.

13 Ibid, 42–43.

14 Ibid, 3, 5.

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

2.12 As the reach of government expanded, however, there was increasing pressure to ask questions about what government was doing. This led to a shift in attitude to official secrecy in the 1960s with the development of a new philosophical and practical approach to government, leading to the description 'open government'.[16] As Greg 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.[17]

2.13 A key principle of open government therefore is accountability—'the indispensable check to be imposed on those entrusted with public power'.[18]

> 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.[19]

2.14 The move to more open government was reflected in the development of 'freedom of information' (FOI) and related administrative laws.

Freedom of information

2.15 Following the introduction of FOI legislation in the United States, the move for such laws was taken up in Australia during the 1960s and 1970s, in speeches, papers and government inquiries,[20] and at both Commonwealth and state levels.[21]

2.16 In 1970, the then Leader of the Opposition, the Hon Gough Whitlam MP, noted with concern that 'excessive secrecy has become commonplace in governmental decision making'.[22] Introduction of FOI legislation became an issue in the lead up to

---

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

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

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

19 Ibid, [3.1.5].

20 See, eg, Interdepartmental Committee on Proposed Freedom of Information Legislation, *Proposed Freedom of Information Legislation* (1974); Interdepartmental Committee on Proposed Freedom of Information Legislation, *Policy Proposals for Freedom of Information Legislation: Report of Interdepartmental Committee* (1976); 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).

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), l, 14.

the 1972 federal election,[23] at which time the Australian Labor Party claimed that the government's monopoly of knowledge had 'led to bad decisions and bad government'.[24]

2.17 The introduction of FOI legislation remained a key political issue during the 1970s. At the same time, other strategies were also pursued to establish a more open system of public administration. In the mid-1970s, the *Ombudsman Act 1976* (Cth), the *Administrative Appeals Tribunal Act 1975* (Cth) and the *Administrative Decisions (Judicial Review) Act 1977* (Cth) were passed. Then in 1982 the *Freedom of Information Act 1982* (Cth) (FOI Act) was added. These legislative reforms—which became known as the 'new administrative law'—aimed to facilitate effective public administration while at the same time safeguarding the civic rights of the individual citizen.[25] As Associate Professor Moira Paterson has noted, FOI laws 'form a vital part of a broader network of laws, both formal and informal, which affect the overall transparency of the executive branch of government'.[26]

2.18 The FOI Act was considered a 'major step in establishing open government' and in overturning 'a deeply entrenched tradition of government secrecy'.[27] The importance of access to information to the accountability of government for its actions was reiterated by Senator the Hon John Faulkner, the then Cabinet Secretary and Special Minister of State, in proposing reforms to the FOI framework in March 2009:

> 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.[28]

---

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) <www.australianpolitics.com/elections/1972> at 23 November 2009.

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

26 Ibid, [1.3].

27 Ibid, 3.

28 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <www.smos.gov.au/speeches/2009/sp_20090324.html> at 26 November 2009.

2.19 By knowing 'whether a government's deeds match its words', open government also helps to provide checks and balances to discourage corruption and misconduct. As commented by the House of Lords in *R v Shayler*:

> Modern democratic government means government of the people by the people for the people. But there can be no government by the people if they are ignorant of the issues to be resolved, the arguments for and against different solutions and the facts underlying those arguments. The business of government is not an activity about which only those professionally engaged are entitled to receive information and express opinions. It is, or should be, a participatory process. But there can be no assurance that government is carried out for the people unless the facts are made known, the issues publicly ventilated. Sometimes, inevitably, those involved in the conduct of government, as in any other walk of life, are guilty of error, incompetence, misbehaviour, dereliction of duty, even dishonesty and malpractice. Those concerned may very strongly wish that the facts relating to such matters are not made public. Publicity may reflect discredit on them or their predecessors. It may embarrass the authorities. It may impede the process of administration. Experience however shows, in this country and elsewhere, that publicity is a powerful disinfectant.[29]

2.20 The relationship between FOI and secrecy provisions—which appear to stand in direct juxtaposition to each other—is a key issue in this Inquiry. Chapter 16 considers in detail the relationship between secrecy provisions and the FOI Act.

Current trends in open government

FOI reforms

2.21 At the time of writing, the FOI Act is the subject of a proposed reform package based on a commitment by the Australian Government to 'undertake the most significant overhaul of the FOI Act since its inception in 1982'.[30] The package includes the *Freedom of Information (Removal of Conclusive Certificates and Other Measures) Act 2009* (Cth), which commenced on 7 October 2009 and two exposure draft bills: the Information Commissioner Bill 2009 and the Freedom of Information Amendment (Reform) Bill 2009 (FOI Exposure Draft Bill).

2.22 The *Freedom of Information (Removal of Conclusive Certificates and Other Measures) Act* represents an important step towards government accountability by removing the barriers to the administrative review of exemption claims that previously arose through the use of 'conclusive certificates'. These permitted a minister or principal officer of an agency to conclusively certify that a document under the FOI Act or the *Archives Act 1983* (Cth) satisfied certain exemptions. Review by the Administrative Appeals Tribunal of the grant of a conclusive certificate was limited to whether there were reasonable grounds for its being issued.

---

29 *R v Shayler* [2003] 1 AC 247, [21].

30 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (Removal of Conclusive Certificates and Other Measures) Bill 2008*, Second Reading Speech, 26 November 2008; Australian Labor Party, *National Platform and Constitution 2009* <www.alp.org.au/platform/index.php> at 7 December 2009, Ch 11.

2.23 More extensive reforms are anticipated in the FOI Exposure Draft Bill: for example, clarifying that the objects of the FOI Act are intended

> 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.[31]

2.24 As discussed in Chapter 16, the FOI Exposure Draft Bill proposes the repeal or amendment of a number of class-based exemptions—that is, documents that are exempt by virtue of their nature: for example, Cabinet documents[32] and electoral rolls.[33] The Exposure Draft would also amend many existing exemptions to make them 'conditional exemptions' subject to a public interest test. Described as being 'weighted in favour of the disclosure of documents', it requires an agency to give access to documents falling within a conditional exemption unless access would, on balance, be contrary to the public interest.[34] Under the new test, factors favouring disclosure in assessing the public interest include: promoting the objects of the Act; informing debate on a matter of public importance; and promoting effective oversight of public expenditure.[35]

2.25 Another important aspect of the FOI Exposure Draft Bill is the information publication scheme set out in sch 2. Under this scheme, agencies are required to publish a range of information on a website, including, for example, information about the agency's structure and functions, and information in documents to which the agency routinely provides to Parliament or in response to FOI requests.[36]

2.26 The Information Commissioner Exposure Draft Bill proposes the establishment of the Office of the Information Commissioner that will bring together the functions for independent oversight of the FOI Act and the *Privacy Act*. The Bill proposes the establishment of the Information Commissioner as head of the office, overseeing the existing role of the Privacy Commissioner, which will be amalgamated into the office, together with the new FOI Commissioner.

---

31 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 1 cl 3.

32 *Freedom of Information Act 1982* (Cth) s 34.

33 Ibid s 47A.

34 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <www.smos.gov.au/speeches/2009/sp_20090324.html> at 26 November 2009.

35 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009).

36 The publication requirement does not include exempt matter or information the publication of which is prohibited by another enactment.

2.27 The Information Commissioner will have a role in reviewing the compliance of agencies with their publication requirements and in promoting the objects of the FOI Act. This extends beyond information access and disclosure to include the management of Commonwealth information for public purposes and as a national resource.[37]

Whole of government information sharing

2.28 The Terms of Reference for this Inquiry acknowledge both the public interest in open and accountable government and the increased need to share Commonwealth information within and between governments and with the private sector. A seamless flow of information within and between governments is referred to as a 'whole of government' approach—'the public administration of the future'.[38] This flow of information, however, may pose particular problems in relation to certain sensitive information, for example, personal information. In the context of such information, the concern is not about 'open government', but rather about the appropriate protection of the information itself in the hands of government officers.

2.29 In its 2004 report, *Connecting Government: Whole of Government Responses to Australia's Priority Challenges*, the Australian Government Management Advisory Committee described the 'whole of government' approach as:

> 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.[39]

2.30 A 'whole of government' approach will normally involve the communication of information between Australian Government agencies. In a submission in response to the Discussion Paper, *Review of Secrecy Laws* (DP 74), the Department of Human Services (DHS) commented on the importance of information sharing to service delivery reform:

> The old model of particular agencies delivering particular programs in particular locations in a fixed way without reference to other Australian Government agencies and programs is changing. Customers are increasingly expecting a different type of service from governments. They expect governments to be proactive and reach out to them with services they are likely to require. They expect not to have to provide the same information to governments time and time again. Customers with special or challenging needs often require intensive case management that brings together information from a range of government programs to provide a holistic response.[40]

---

37 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 1 cl 3(3). See also Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).

38 Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia's Priority Challenges* (2004), vi.

39 Ibid, 4. The Management Advisory Committee is a forum of 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> at 23 November 2009.

40 Department of Human Services, *Submission SR 83,* 8 September 2009.

2.31 Wherever information-sharing objectives arise, a parallel concern is the role of secrecy provisions, or other mechanisms, to protect that information in appropriate circumstances. Ensuring that channels for the communication of protected information are built into, or complement, secrecy provisions may be crucial to achieving an appropriate balance between protecting information and providing effective service delivery. As noted by the DHS in relation to the wide range of personal information collected and managed by their agencies:

> While the appropriate protection of personal information about customers must, of course, remain paramount, it is essential that secrecy provisions complement and assist, rather than frustrate, improvements to service delivery.[41]

2.32 New technologies can be used to facilitate a 'whole of government' approach to sharing information. An example is 'Government 2.0', which is discussed in the next section.

Government 2.0

2.33 'Government 2.0' refers to the application of Web 2.0[42] to facilitate access to public sector information, as well as encouraging online engagement with government initiatives. Reflecting these goals, the Australian Government has established the Government 2.0 Taskforce to provide advice and assistance on:

- making government information more accessible and usable;
- making government more consultative, participatory and transparent, including maximising the extent to which government utilises the views, knowledge and resources of the general community;
- building a culture of online innovation within government; and
- promoting collaboration across agencies with respect to online and information initiatives.[43]

2.34 Also included in the Taskforce's terms of reference is the identification and trial of initiatives that may achieve or demonstrate how the above objectives may be accomplished. For example, the ALRC is receiving funding through the Taskforce for the purpose of trialling a closed online focus group as a consultation strategy for its inquiry into family violence.[44]

---

41 Ibid.

42 Web 2.0 can be seen as principles or practices that facilitate interactive online information sharing and collaboration.

43 Government 2.0 Taskforce, *Towards Government 2.0: An Issues Paper* (2009).

44 Terms of Reference, 17 July 2009. See <http://www.alrc.gov.au/.html> at 23 November 2009.

2.35 On 23 July 2009, the Taskforce released *Towards Government 2.0: an Issues Paper*.[45] Many of the questions asked by the Taskforce have relevance to the ALRC's Inquiry into secrecy laws, including, for example:

- what are the ways in which we build a culture within government which favours the disclosure of public sector information, and what barriers restrict or complicate this;[46]
- what government information should be more freely available;[47] and
- what are the possible privacy, security, confidentiality or other implications that might arise in making public sector information available?[48]

2.36 Since the potential to share knowledge and information initiatives across government relies on 'the interoperability of information and business architectures', the Taskforce has also asked what approaches the Australian Government should use to allow information to be shared easily between government agencies and between such agencies and their users.[49] The Taskforce is due to deliver its final report to the Australian Government on 31 December 2009.

Freedom of expression

2.37 While open government is central to this Inquiry, another key principle of relevance is freedom of expression. This section of the chapter considers the international and domestic laws that protect this freedom, including the ICCPR and rights enacted in domestic law. It goes on to discuss the relationship between secrecy provisions and freedom of expression, including protection for 'public interest disclosures'.

International Covenant on Civil and Political Rights

2.38 The ICCPR, described as 'one of the most important human rights conventions of the United Nations era',[50] was adopted by the United Nations General Assembly on 16 December 1966 and ratified by the Australian Government in 1980. In the context of this Inquiry, the key provision is art 19:

> 1. Everyone shall have the right to hold opinions without interference.
>
> 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of

45 Government 2.0 Taskforce, *Towards Government 2.0: An Issues Paper* (2009).
46 Ibid, Question 2.
47 Ibid, Question 3.
48 Ibid, Question 4.
49 Ibid, Question 8.
50 B Opeskin and D Rothwell (eds), *International Law and Australian Federalism* (1997), 16.

> frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
>
> 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
>
> (a) For respect of the rights or reputations of others;
>
> (b) For the protection of national security or of public order (*ordre public*), or of public health or morals.[51]

2.39 The Human Rights Committee of the United Nations (Human Rights Committee) has commented that the right to freedom of expression includes:

> Not only freedom to impart information and ideas of all kinds but also freedom to seek and receive them regardless of frontiers and in whatever medium, either orally, in writing or in print, in the form of art, or through any other media of his choice.[52]

2.40 The right set out in art 19(2) is qualified by the provisions in art 19(3)—that freedom of expression may be subject to 'certain restrictions'. In its general comment on art 19, the Human Rights Committee stated that:

> Paragraph 3 expressly stresses that the exercise of the right to freedom of expression carries with it special duties and responsibilities and for this reason certain restrictions on the right are permitted which may relate either to the interests of other persons or to those of the community as a whole. However, when a State party imposes certain restrictions on the exercise of freedom of expression, these may not put in jeopardy the right itself. Paragraph 3 lays down conditions and it is only subject to these conditions that restrictions may be imposed: the restrictions must be 'provided by law'; they may only be imposed for one of the purposes set out in subparagraphs (a) and (b) of paragraph 3; and they must be justified as being 'necessary' for that State party for one of those purposes.[53]

2.41 How do secrecy provisions—that appear to restrict freedom of expression—sit within the framework of art 19? The *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights* state that any such limitations on the ICCPR must: be recognised by the relevant article of the ICCPR; respond to a pressing public or social need; pursue a legitimate aim; and be proportionate to that aim.[54] The principles also state that the expression 'public order',

---

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

52 United Nations Human Rights Committee, *General Comment No 10: Freedom of Expression (Art 19)*, HRI/GEN/1/Rev.9/Vol.1 (1983).

53 Ibid.

54 United Nations Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4 (1984). The principles were developed by a group of experts for consideration by the United Nations Commission on Human Rights and the Human Rights Committee.

as used in the ICCPR, 'may be defined as the sum of rules which ensure the functioning of society or the set of fundamental principles on which society is founded'. This expression is not limited to criminal law enforcement in the context of the ICCPR and includes, for example, respect for human rights.[55]

2.42 The Human Rights Committee is responsible for monitoring compliance with the ICCPR. To date, Australia has submitted five reports, each providing an account of the development of legislation, administration and practice relevant to each article of the ICCPR over the time covered by each report.

2.43 In relation to art 19, Australia's third report included reference, for example, to the FOI Act as enabling members of the public to request access to information in the possession of the Australian Government.[56] The third report also noted the secrecy obligations resting on Australian public servants:

> All Australian jurisdictions require their civil servants to keep confidential information relating to their work, duties and responsibilities. The Federal Government and some state governments also impose restrictions on public comment by civil servants.[57]

2.44 Australia is also a signatory to the First Optional Protocol to the ICCPR. The Protocol allows individuals within Australia, who claim that their rights under the ICCPR have been violated, to submit a written complaint to the Human Rights Committee. Before submitting a complaint, the individual must have exhausted all domestic remedies. The Human Rights Committee publishes its 'views' on the complaint after consulting the state party on the matter. It is possible, therefore, for Australians who claim that their rights under art 19 have been violated to seek the views of the Committee on their individual case.

The protection of human rights in domestic law

2.45 In the domestic context, human rights may be protected in a number of ways: in the *Australian Constitution*; through an instrument, such as a Charter of Rights; through individual statutory protection; and/or through a combination of common law and statute.

2.46 Australia does not have a federal human rights statute, such as a 'Bill of Rights' or 'Charter of Rights'. In comparison, New Zealand introduced a *Bill of Rights* in 1990; the United Kingdom passed the *Human Rights Act* in 1998; and ACT and Victoria introduced, respectively, the *Human Rights Act 2004* (ACT) and the *Charter*

---

55 Ibid. Other permissible restrictions on the right to freedom of expression found in the ICCPR—those necessary to protect national security, public health, public morals, and the rights and reputations of others—are discussed in detail in Chs 5, 8.

56 *International Covenant on Civil and Political Rights: Third Periodic Reports of States Parties Due in 1991, Addendum: Australia*, CCPR/C/AUS/98/3 (1999), [1027].

57 *International Covenant on Civil and Political Rights: Fourth Periodic Reports of States Parties Due in 1996: Australia*, CCPR/C/AUS/98/4 (1999), [1016]–[1017].

of Human Rights and Responsibilities Act 2006 (Vic). Each of these formal instruments includes an express protection of freedom of expression.[58]

2.47 On 10 December 2008, the Australian Government established a Committee, chaired by Fr Frank Brennan SJ to conduct a nationwide consultation aimed at

> finding out which human rights and responsibilities should be protected and promoted in Australia, whether human rights are sufficiently protected and promoted, and how Australia could better protect and promote human rights.[59]

2.48 The Committee reported on 30 September 2009 and recommended the introduction of a Human Rights Act as a step, among other things, to 'improve the quality and accountability of government'.[60]

2.49 While Australia does not have a general statute at the federal level protecting human rights, some human rights are protected, for example, in the *Australian Constitution*[61] and specific statutes, such as the: *Racial Discrimination Act 1975* (Cth); *Sex Discrimination Act 1984* (Cth); *Australian Human Rights Commission Act 1986* (Cth); *Disability Discrimination Act 1992* (Cth); and *Age Discrimination Act 2004* (Cth). In addition to such express provisions, courts may interpret legislation in a manner that seeks to uphold human rights.[62]

2.50 In what have been called the 'free speech cases', the High Court has held that the system of representative and responsible government established by the *Australian Constitution* implies a commitment to the freedom of political communication.[63] In one of the first decisions of the High Court in this context, Mason CJ commented on its relationship to open and accountable government:

> Indispensable to that accountability and that responsibility is freedom of communication, at least in relation to public affairs and political discussion. Only by exercising that freedom can the citizen communicate his or her views on the wide range of matters that may call for, or are relevant to, political

---

58 *Human Rights Act 1998* (United Kingdom) s 12; *Bill of Rights 1990* (New Zealand) s 14; *Human Rights Act 2004* (ACT) s 16; *Charter of Human Rights and Responsibilities 2006* (Vic) s 15.

59 National Human Rights Consultation Committee, *National Human Rights Consultation—Report* (2009), xiii.

60 Ibid, xvii.

61 The rights in the *Australian Constitution* include: trial on indictment of any offence against any law of the Commonwealth shall be by jury (s 80); any property acquired by the Commonwealth Government must be acquired on just terms (s 51(xxxi)); the Commonwealth Government shall not make any law to establish any religion or to interfere with religious freedom (s 116); citizens are not to be subjected to any discrimination in any State by reason of residence in another State (s 117); and government actions are subject to judicial review (s 75(v)).

62 *Coco v The Queen* (1993) 179 CLR 427, 437–438.

63 *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.

> action or decision. Only by exercising that freedom can the citizen criticize government decisions and actions, seek to bring about change, call for action where none has been taken and in this way influence the elected representatives.[64]

2.51 In *Lange v Australian Broadcasting Corporation* (*Lange*),[65] the High Court affirmed that there is an implied freedom in the *Australian Constitution* to publish material discussing governmental and political matters, and that the common law of defamation must conform to these requirements.[66] The Court stated, however, that laws could be passed to limit that freedom 'to satisfy some other legitimate end',[67] provided two questions were satisfactorily answered:

> First, does the law effectively burden freedom of communication about government or political matters either in its terms, operation or effect? Second, if the law effectively burdens that freedom, is the law reasonably appropriate and adapted to serve a legitimate end 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.[68]

2.52 While not as broad as a general right to freedom of expression, the implied guarantee of freedom of political communication amounts to a restriction on the legislative and executive power of the Commonwealth.

Freedom of expression and secrecy provisions

2.53 By restricting Commonwealth officers and others from communicating government information, secrecy provisions limit freedom of expression in certain respects. Their legitimacy, therefore, must be tested internationally against the backdrop of the ICCPR, and domestically against the implied freedom of political communication.

2.54 An instructive illustration outside Australia is the case of *R v Shayler*, in which the House of Lords considered whether a provision of the *Official Secrets Act 1989* (UK) breached art 10 of the *European Convention on Human Rights,* which guarantees the right to freedom of expression among member states.[69] Section 1(1) of the *Official Secrets Act* makes it an offence for a current or former member of the security or intelligence services to disclose information relating to security or intelligence without lawful authority.

2.55 The House of Lords found that the secrecy provision was not incompatible with the right to freedom of expression, even though the offence was broadly framed, did

---

64 *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, 138.
65 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
66 Ibid, 556.
67 Ibid, 562.
68 Ibid, 567–568.
69 *R v Shayler* [2003] 1 AC 247.

not include a public interest defence, and, unlike other provisions of the *Official Secrets Act,* did not require that the disclosure be 'damaging'.[70] The House of Lords considered that the *Official Secrets Act* included 'sufficient and effective safeguards' to allow a person to communicate information—including a reviewable process of official authorisation for disclosures and avenues for complaint about maladministration.[71] On this basis their Lordships concluded that the interference with freedom of expression was necessary to achieve the legitimate object of protecting national security.[72]

2.56 In Australia, the breadth of s 70 of the *Crimes Act 1914* (Cth) and the secrecy regulation under the now repealed *Public Service Act 1922* (Cth) was identified as an issue in the context of the ICCPR when, in the third report on compliance with art 19 in 1999, Australia noted that such provisions 'effectively prohibit the disclosure of all information by a federal public servant other than in the course of the officer's official duty'.[73] The report also referred to the conclusions of the review of federal criminal laws by the Committee chaired by Sir Harry Gibbs (the Gibbs Committee) in 1991 and particularly the comment by the Committee that '[t]he catchall provisions of the existing law are wrong in principle and additionally ... they are seriously defective from the point of view of effective law enforcement'.[74]

2.57 The context for assessing the validity of secrecy provisions in Australia is the implied guarantee of freedom of political communication in the *Australian Constitution*. In 2003, the matter arose in *Bennett v President, Human Rights and Equal Opportunity Commission* (*Bennett*).[75] Peter Bennett, a public servant employed by the Australian Customs Service and President of a registered industrial organisation representing customs officers, publicly advocated the establishment of a Single Border Protection Agency and commented in the media on other customs matters. The Chief Executive Officer of Customs issued Bennett with a formal direction not to make comments in the media 'about public business or anything of which you have official knowledge'.[76] After Bennett made comments in a radio interview about proposed cuts to waterfront officers, he was disciplined for breach of the now repealed reg 7(13) of the *Public Service Regulations 1999* (Cth):

> 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.

---

70 Ibid, 276–277.
71 Ibid, 275.
72 Ibid.
73 *International Covenant on Civil and Political Rights: Third Periodic Reports of States Parties Due in 1991, Addendum: Australia*, CCPR/C/AUS/98/3 (1999), [1016]–[1017].
74 Ibid, [1024]. H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.4].
75 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.
76 Ibid, [12].

2.58 Bennett's formal complaint to the Human Rights and Equal Opportunity Commission, alleging discrimination and breach of his right to freedom of expression, was unsuccessful. He sought review in the Federal Court, arguing that reg 7(13) was invalid as it infringed the implied constitutional freedom of political communication.

2.59 Finn J held that reg 7(13) was inconsistent with the implied freedom of political communication and declared it to be invalid. In doing so, he applied the two-limbed test set out in *Lange,* quoted above.[77] On the first limb, Finn J held that, as reg 7(13) controlled the disclosure by public servants of information about the 'public business' of the Australian Government, it effectively burdened freedom of political communication. Finn J then considered, under the second limb, whether the regulation was reasonably appropriate and adapted to serve a legitimate end compatible with maintaining the Australian system of representative and responsible government. He held that, while there may be public interests, or 'legitimate ends', that justify the burden that secrecy provisions impose on freedom of political communication—including national security, cabinet confidentiality, protection of privacy and the maintenance of an impartial and effective public service—a 'catch-all' provision that did not differentiate between the types of information protected or the consequences of disclosure went too far:

> 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.[78]

2.60 Following the decision in *Bennett,* reg 7(13) of the *Public Service Regulations* was repealed and replaced by reg 2.1.[79] The latter is expressly limited to situations in which it is reasonably foreseeable that the disclosure of official information could be prejudicial to the effective working of government.[80] The constitutional validity of this new regulation was challenged in *R v Goreng Goreng*.[81] In that case, Refshauge J of the Supreme Court of the Australian Capital Territory considered that, unlike former reg 7(13), reg 2.1 was not a 'catch-all' provision, but much more limited and targeted to the protection of a legitimate public interest in the effective working of government.[82]

---

77 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520, 567–568.
78 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [98]–[99].
79 *Public Service Amendment Regulations (No 1) 2006* (Cth). The text of reg 2.1 is set out in Appendix 5.
80 *Public Service Regulations 1999* (Cth) reg 2.1(3).
81 *R v Goreng Goreng* [2008] ACTSC 74.
82 Ibid, [37]. The operation of reg 2.1 is considered in Ch 12.

Public interest disclosure

2.61 A freedom to discuss governmental and political matters may include calling the government to account, for example in relation to allegations of mismanagement and even corruption. The legitimacy of such 'public interest disclosures'—colloquially known as 'whistleblowing' is a key concern in the context of secrecy provisions. Are there circumstances in which a Commonwealth officer, or others, should be immune from punishment for breach of secrecy obligations, for disclosing information 'in the public interest'.

2.62 The nature of the problem, and the key issues involved, are illustrated by the following case study:

Case study: *R v Kessing*[83]

Allan Kessing was employed as a customs officer with the Australian Customs Service (ACS) until his resignation on 10 May 2005. Kessing signed an 'Official Secrets' form in which he acknowledged his understanding that all official information he had acquired in the course of employment was not to be published or communicated to any unauthorised person. While at the ACS, Kessing had worked on two reports regarding criminal activity and organised crime at Sydney airport. The reports were classified 'Highly Protected'[84] and shared only within the ACS. On 31 May 2005, an article appeared in *The Australian* newspaper describing lax security at Sydney airport and citing information contained in the ACS reports. As a result, an expert review of airport security was commissioned, resulting in a government commitment to improving airport security.[85]

Kessing was charged with disclosing the information in the reports in contravention of s 70(2) of the *Crimes Act*. Kessing denied communicating the information. Defence counsel argued that, even if Kessing were found to have committed the offence, he could claim that he had a lawful justification or excuse, that the public had an interest in being made aware of the information.

Kessing was found guilty. In sentencing, Bennett SC DJC commented that:

> Accepting that it is in the public interest to expose the inadequacy of an agency or government manifested by its failure to respond in a timely fashion to an internal report generated at the lower levels of the organisation to inform management of operational and related concerns, that is an entirely different matter from the

83 *R v Kessing* (2008) 73 NSWLR 22; *Kessing v The Queen* [2008] NSWCCA 310.
84 The security classification scheme used by the Australian Government is discussed in Ch 14.
85 J Wheeler, *Airport Security—Report by the Rt Hon Sir John Wheeler JP DL* (2002).

> unauthorised dissemination of the information harvested in the course of operational activities and the intelligence developed therefrom, upon which the report was generated, such as has occurred in this instance.
>
> Whether or not it is appropriate to view the offender in the heroic light with which he has been bathed by some for having exposed what he represents to be inadequate aspects of management within the Australian Customs Service concerned with Sydney Airport, there was no justification whatsoever for the communication of the content of these reports.[86]

2.63 In commenting on this case, the House of Representatives Standing Committee on Legal and Constitutional Affairs noted that:

> Much attention was focused on the apparent irony that Mr Kessing ended up with a criminal record but the leak resulted in a major review of airport safety and security by Sir John Wheeler after which the Government implemented a $200 million package to improve airport security. In some circles, Mr Kessing is considered a 'hero'. …
>
> Informal reporting is normal and acceptable, but there must be a reporting scheme that opens pathways to bypass line management and to formalise matters of concern. In this case, such a scheme could have provided an opportunity to press the issues of concern directly to senior management or to an oversight agency.[87]

2.64 The following section considers the status of public interest disclosures at the federal level, and the relationship between such disclosures and this Inquiry.

Public interest disclosure legislation

2.65 Currently, there is some protection at the Commonwealth level for people who make public interest disclosures. As discussed in Chapter 12, s 16 of the *Public Service Act 1999* (Cth), called '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 APS Commissioner, Merit Protection Commissioner or the head of an agency. This provision is quite limited in scope. Importantly, it does not provide protection from 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.[88]

---

86 *R v Kessing* (2008) 73 NSWLR 22, [59]–[60].

87 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Inquiry into Whistleblowing Protections Within the Australian Government Public Sector* (2009), 116.

88 A Brown, *Public Interest Disclosure Legislation in Australia* (2006), 34.

2.66 Some Commonwealth legislation contains more comprehensive protection for whistleblowers working in particular areas. These provisions are considered in Chapter 10. In addition, all Australian states and territories have enacted legislation to facilitate the making of public interest disclosures and to protect people who make them.[89] 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'.[90]

Whistleblower Protection report

2.67 In February 2009, the House of Representatives Standing Committee on Legal and Constitutional Affairs (Standing Committee) issued a report called *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (the *Whistleblower Protection* report).[91] The Standing Committee recommended that the Australian Government introduce public interest disclosure legislation to provide whistleblower protections in the Australian Government public sector.[92] The proposed legislation would establish a system whereby Commonwealth employees could make disclosures about 'serious matters' within their organisation, to other public service agencies or, in limited circumstances, publicly.

2.68 The Standing Committee recommended that the proposed legislation cover a broad range of participants in the Australian Government, including:

- Australian Government and general government sector employees, including Australian Public Service employees and employees of agencies under the *Commonwealth Authorities and Companies Act 1997*;
- contractors and consultants engaged by the public sector;
- employees of contractors and consultants engaged by the public sector;
- Australian and locally engaged staff working overseas;
- members of the Australian Defence Force and Australian Federal Police;
- parliamentary staff;

---

89 *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).

90 *Whistleblowers Protection Act 2001* (Vic) s 15.

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

92 Ibid, Rec 1.

- former employees in one of the above categories; and
- anonymous persons likely to be in one of the above categories.[93]

2.69 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.[94] A person making a disclosure would need to have an honest and reasonable belief, on the basis of information available to them, that the matter concerns 'disclosable' conduct under the legislation.[95]

2.70 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 externally (to the Commonwealth Ombudsman, the APS Commissioner or other integrity agency) or both.[96]

2.71 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), civil liability and administrative penalties.[97]

2.72 The Standing Committee also considered that it was necessary to protect a person making a public interest disclosure to third parties—such as 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.[98]

2.73 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

93 Ibid, Rec 3.
94 Ibid, Rec 7.
95 Ibid, Rec 10.
96 Ibid, Recs 15–19.
97 Ibid, Rec 14.
98 Ibid, [8.72]–[8.73].

> the public sector may not adequately handle an issue and that a subsequent disclosure to the media could serve the public interest.[99]

2.74 The Standing Committee's final recommendation, however, 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, and the matter threatened immediate serious harm to public health or safety.[100]

2.75 The recommendation relating to disclosures to third parties has been criticised as being too limited. Brown, for example, 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 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'.[101]

2.76 In a submission to this Inquiry, Brown stated that the proposed approach

> 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.[102]

2.77 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).[103]

---

99 Ibid, [8.77].
100 Ibid, Rec 21.
101 Ibid.
102 AJ Brown, *Submission SR 44,* 18 May 2009.
103 Ibid.

2.78 At the time of writing, the Australian Government had not responded to the *Whistleblower Protection* report, although the Government has indicated that it intends to develop public interest disclosure legislation in 2009.[104] Given the recent Standing Committee inquiry and report, and the Government commitment to introduce public interest disclosure legislation, the ALRC has confined its consideration in this Report to the interaction between the proposed public interest disclosure legislation and secrecy laws. This issue is discussed in Chapters 7 and 10.

2.79 The ALRC does, however, reaffirm its recommendations made in previous reports that the Australian Government should legislate to introduce a comprehensive public interest disclosure scheme covering all Australian Government agencies.[105] In the ALRC's view, a robust public interest disclosure regime is an essential element in an effective system of open government. For the purposes of this Report, the ALRC is proceeding on the basis that such legislation will be put in place and that it 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.

Balancing secrecy, freedom of expression and open government

2.80 The challenge for the ALRC in this Inquiry is to strike the right balance between the public interest in open and accountable government and the public interest in maintaining the confidentiality of some government information. The goal, then, is to identify the proper place, if any, for secrecy provisions in the context of a system of open and accountable government—consistent with Australia's obligations under international law.

2.81 The appropriate role for secrecy provisions in an era of open government was acknowledged from the outset during the debate about FOI laws in the 1970s. 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 with that underlying secrecy provisions.[106] The Senate Standing Committee also criticised what it then described as 'a fashionable contemporary drafting practice':

---

104 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <www.smos.gov.au/speeches> at 6 December 2009.

105 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 3–1; Australian Law Reform Commission, *Integrity: But Not by Trust Alone: AFP & NCA Complaints and Disciplinary Systems*, ALRC 82 (1996), Rec 117.

106 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.

> 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.[107]

2.82 The conflict between the secrecy required of Commonwealth officers and open government—as a philosophy of government—remains today. For the individual Commonwealth officer this may generate uncertainties:

> 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.[108]

2.83 In this Report, the ALRC makes a number of recommendations aimed at clarifying the obligations of confidentiality imposed on Commonwealth officers and others handling government information. Reflecting the commitment towards openness expressed in recent policy initiatives of the Australian Government, including Government 2.0 and the proposed reforms relating to the FOI Act, the ALRC also recommends the reform of secrecy laws so that unauthorised disclosures are only criminalised in circumstances where the disclosure causes, or is likely or intended to cause, harm to an essential public interest.

2.84 The recommendations also reflect Australia's international obligations under the ICCPR. The *Australian Law Reform Commission Act 1996* (Cth) expressly directs the ALRC that in performing its functions 'the Commission must have regard to all of Australia's international obligations' that are relevant to the matter in the Terms of Reference.[109] In particular, the ALRC 'must aim at ensuring that the laws, proposals and recommendations it reviews, considers or makes', are, 'as far as practicable' consistent with the ICCPR.[110]

2.85 In this Inquiry, the ALRC recommends a new and principled framework that strikes a fair balance between the public interest in open and accountable government and protecting essential public interests—such as national security, defence, law enforcement and investigation, and public safety. This requires a focus on the idea of the public interest, both in the general sense of an overriding justification for government action 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.

---

107 Ibid, 233.
108 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 94.
109 *Australian Law Reform Commission Act 1996* (Cth) s 24(2).
110 Ibid s 24(1)(b).

3. Overview of Current Secrecy Laws

Contents

Introduction

3.1 The ways in which individuals use and disclose government information is subject to several layers of regulation. This chapter provides an overview of current laws governing the disclosure of government information by individuals within and beyond the Australian Government.

3.2 This chapter first considers the equitable duty of confidence and common law duties of loyalty and fidelity and the impact of these duties on the use and disclosure of government information. Secondly, the chapter examines the secrecy provisions contained in Commonwealth legislation with a view to identifying points of commonality and difference between them. Finally, the chapter discusses the general criminal offences in ss 70 and 79(3) of the *Crimes Act 1914* (Cth), which apply criminal sanctions to the breach of secrecy obligations.

Duties of confidentiality and loyalty and fidelity

Breach of confidence

3.3 The equitable action for breach of confidence may be used to restrict the disclosure of information in certain circumstances. 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'.[1]

3.4 An action for breach of confidence may be brought to restrain disclosure by a third party who has received confidential information. The information may have been communicated in breach of a duty of confidence,[2] or may have come into the hands of the third party by human error.[3]

3.5 While legal actions for breach of confidence most commonly relate to commercial or technical information held by private individuals and companies, the principles of breach of confidence can be applied to protect government information in some circumstances.[4] However, different principles apply to restraining the disclosure of government information.

3.6 The leading case in this area is *Commonwealth v Fairfax,*[5] in which the Commonwealth sought an injunction to prevent two Australian newspapers from publishing extracts from an upcoming book, *Documents on Australian Defence and Foreign Policy 1968–1975*.[6] The extracts included parts of classified government documents concerning international treaties, foreign intelligence services and military bases. Early editions of the newspapers had been distributed before the publishers received notice of the interim injunction restraining publication.

3.7 The High Court held that the disclosure of confidential government information would only be restrained if 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'.[7] The test set out in *Commonwealth v Fairfax* involves balancing the public interest in knowing and discussing government actions with the need to protect confidentiality. As noted by Mason J:

> 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.

---

1 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50, citing Swinfen Eady LJ in *Lord Ashburton v Pope* (1913) 2 Ch 469, 475.

2 See, eg, *Commonwealth v Fairfax* (1980) 147 CLR 39, 50–51 in which 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.

3 See, eg, *Victoria v Nine Network* (2007) 19 VR 476.

4 *Commonwealth v Fairfax* (1980) 147 CLR 39, 51.

5 Ibid.

6 G Munster and J Walsh, *Documents on Australian Defence and Foreign Policy 1968–1975* (1980).

7 *Commonwealth v Fairfax* (1980) 147 CLR 39, 52.

> 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.[8]

3.8 In *Commonwealth v Fairfax,* the Court considered that the degree of embarrassment to Australia's foreign relations that would flow from disclosure was not enough to justify protection of the information. The Court also took account of the fact that sales of the book had already been made, and some extracts already published, which meant that any detriment would not be avoided by the grant of an injunction.[9]

3.9 The public interest test set out in *Commonwealth v Fairfax* places the burden on governments to justify the maintenance of the confidentiality of the information. The reason for this is the importance of freedom of communication and public discussion. As McHugh J explained in *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd*:

> governments act, or at all events are constitutionally required to act, in the public interest. Information is held, received and imparted by governments, their departments and agencies to further the public interest. Public and not private interest, therefore, must be the criterion by which Equity determines whether it will protect information which a government or governmental body claims is confidential.[10]

3.10 Balancing the public interests in confidentiality, on the one hand, and freedom of information and discussion on the other, will lead to different results depending on the type of information under consideration. In *Victoria v Nine Network,* the Supreme Court of Victoria restrained the publication of information contained in documents inadvertently mislaid by the government agency responsible for the state's prisons. The Court determined the 'overwhelming public interest' was to maintain the confidentiality of a patient profile and psychiatric information about a prisoner who had made allegations of sexual misconduct.[11] However, the Court did not restrain the publication of other documents relating to investigation plans, the reports of investigations and general information about lock-up procedures where there were no questions about privacy or operational sensitivities.[12]

3.11 A statutory duty of confidentiality may arise where legislation confers power on a person or agency to obtain information. In the case of *Johns v Australian Securities Commission,* the High Court held that a statute that confers a power to obtain information for a particular purpose limits, expressly or impliedly, the purposes for which that information can then be used or disclosed. As such, the person obtaining information in exercise of a statutory power must treat the information as

---

8 Ibid, 52.

9 Ibid, 54. The High Court did, however, grant an injunction to restrain infringement of the Commonwealth's copyright in documents that it had brought into existence.

10 *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86, 191.

11 *Victoria v Nine Network* (2007) 19 VR 476, [84].

12 Ibid, [122]; [146]; [160].

confidential.[13] Even though this duty of confidentiality is imposed by statute, the equitable remedy of injunction is available to enforce the duty against a public authority.[14]

3.12 A duty of confidentiality akin to that which arises in private commercial contracts may also apply where government has a contractual relationship with a private provider of a government service (for example, a provider of an aged care service).[15] An obligation of confidence may arise because of the circumstances in which the information is imparted or because of an express confidentiality clause in a contract.[16]

Duty of loyalty and fidelity

3.13 The common law imposes a duty of loyalty and fidelity upon all employees. This duty arises from the contract of employment,[17] but may also arise from a fiduciary obligation where the employee is in a special position of trust and confidence.[18] In the context of confidential information, the duty of fidelity requires that an employee must not use information obtained in the course of his or her employment to the detriment of the employer.[19]

3.14 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.[20] Finn noted that the formulation of the duty is necessarily imprecise because of the variety of issues to be considered before using government information, 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.[21]

3.15 Some years later, in *Bennett v President, Human Rights and Equal Opportunity Commission*, Finn J made a number of observations about whether a duty not to disclose information could be supported by a public servant's duty of loyalty and

---

13 *Johns v Australian Securities Commission* (1993) 178 CLR 408, 424.
14 Ibid.
15 J Macken, P O'Grady, C Sappideen and G Warburton, *Law of Employment* (4th ed, 2002), 141.
16 Confidentiality clauses are now included in many government 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. Confidentiality clauses in government contracts are discussed in Ch 13.
17 *Robb v Green* [1895] 2 QB 315.
18 J Macken, P O'Grady, C Sappideen and G Warburton, *Law of Employment* (4th ed, 2002), 139–141.
19 *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 625–628.
20 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 204.
21 Ibid, 205–206.

fidelity. Finn J 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.[22]

3.16 Finn J referred to Canadian jurisprudence and particularly the conclusion of the Supreme Court of Canada in *Fraser v Public Service Staff Relations Board*.[23] Mr Fraser was a public servant who was dismissed after making public comments critical of government policy. In deciding whether the dismissal was justified, the Supreme Court balanced 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.[24]

3.17 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.[25]

3.18 However, the right to comment is not unqualified. Restrictions on the right of public servants to comment on government matters may be based on the level of seniority of the public servant, or participation in policy development or managerial decisions.[26]

3.19 As Finn J noted in *Bennett*, there is little law on how the duty of fidelity applies to public servants in Australia. Because the Canadian principles have been developed

---

22 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, [125].
23 *Fraser v Public Service Staff Relations Board* [1985] 2 SCR 455.
24 Ibid, [34].
25 Ibid, [41].
26 *Osborne v Canada* [1991] 2 SCR 69, 99.

in the context of a Charter of Human Rights that protects freedom of speech, they may not be readily applicable to the Australian context.

Specific statutory secrecy provisions

3.20 Secrecy provisions contained in Commonwealth legislation are many and varied. As noted 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 Commonwealth information. The ALRC has identified 506 secrecy provisions in 176 pieces of primary and subordinate legislation. A table of secrecy provisions in Commonwealth legislation is set out in Appendix 5.

3.21 Approximately 70% of the statutory secrecy provisions identified create criminal offences. Around 75% of these offences are indictable offences—that is, offences punishable by imprisonment for a period exceeding 12 months.[27] 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.[28]

3.22 Some secrecy provisions do not expressly impose criminal penalties for breach, but rather impose a duty of confidentiality on individuals. For example, the secrecy provision in the *Australian Hearing Services Act 1991* (Cth) provides that

> it is the duty of a person who is a Director, a member of the staff of the Authority, a member of a committee or a person engaged as a consultant under section 50 not to disclose any information that has been acquired by the person because of being such a Director, member or consultant.[29]

3.23 While provisions of this kind are not, in themselves, offences, s 70 of the *Crimes Act 1914* (Cth) may attach criminal sanctions to the breach by a Commonwealth officer of this kind of 'duty not to disclose'.[30] In this way, specific secrecy provisions—that do not themselves create an offence—interact with general offences in the *Crimes Act* to criminalise the disclosure of some information by Commonwealth officers.

3.24 The remaining non-criminal secrecy provisions establish rules for the handling of certain information by officers or agencies. For example, s 41(2) of the *Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989* (Cth) provides that the Institute or Council shall not disclose information if that disclosure would be inconsistent with the views or sensitivities of relevant Aboriginal persons or Torres Strait Islanders. As discussed in Chapter 1, the ALRC has taken the view that only those provisions that *prohibit* the disclosure of information are secrecy provisions.

---

27 *Crimes Act 1914* (Cth) s 4G.
28 Ibid s 4H.
29 *Australian Hearing Services Act 1991* (Cth) s 67(1).
30 Section 70 is discussed in detail later in this chapter.

3.25 Statutory secrecy provisions exhibit four common elements:

- protection of particular kinds of information;
- regulation of particular persons;
- prohibition of certain kinds of activities in relation to the information; and
- exceptions and defences which set out the circumstances in which a person does not infringe a secrecy provision.

3.26 It is notable that this list of the common elements of secrecy provisions does not include an express requirement that the disclosure cause or be likely to cause harm. Only a small number of statutory secrecy offences expressly include such a harm element. For example, the *Defence Force Discipline Act 1982* (Cth) requires that, for an offence to have been committed, the unauthorised disclosure of information must be 'likely to be prejudicial to the security or defence of Australia'.[31]

3.27 The following section examines each of these elements in turn. It provides examples of the different approaches taken across Commonwealth legislation to the protection of official information, and draws attention to the kinds of interests that secrecy provisions seek to protect from harm. Where relevant, the proportion of secrecy provisions that exhibit particular variations is noted.[32]

What kind of information is protected?

3.28 Secrecy provisions in Commonwealth legislation prohibit the unauthorised handling of various kinds of information. The information protected by secrecy provisions can be considered in accordance with the following six categories:

- any information;
- confidential information;
- personal information;
- commercial information;
- information relating to an investigation; and
- other types of information.

---

31 *Defence Force Discipline Act 1982* (Cth) s 58(1).

32 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 secrecy offences alone.

Any information

3.29 Approximately 15% of secrecy provisions in Commonwealth legislation relate to the unauthorised disclosure or use of *any* information. These provisions typically cover any information obtained by a person during the course of his or her employment.[33] Generally, these provisions prohibit the disclosure of any information obtained by a person carrying out, performing or exercising duties, functions or powers under:

- 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.

3.30 Australian Public Service (APS) employees are subject to the APS Code of Conduct, set out in s 13 of the *Public Service Act 1999* (Cth), which imposes a number of duties on APS employees that limit the disclosure of official information. In particular, the Code of Conduct requires an employee to behave honestly and with integrity in the course of his or her employment,[34] and to maintain appropriate confidentiality about dealings the employee has with any minister or minister's member of staff.[35]

3.31 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 1999* (Cth) 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.

3.32 Legislation establishing a statutory authority or independent agency may also include a similar secrecy provision to cover the employees of that authority or agency.[36]

---

33 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).

34 *Public Service Act 1999* (Cth) s 13(1).

35 Ibid s 13(6).

36 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 207(1); *Australian Human Rights Commission Act 1986* (Cth) s 49(1); *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2).

3.33 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.

Confidential information

3.34 About 8% of secrecy provisions identified by the ALRC 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.[37] Others prohibit the disclosure of information that was supplied 'in confidence'.[38] The most general provision of this kind is reg 2.1(4) of the *Public Service Regulations*:

> 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.

3.35 Provisions covering boards and committees also tend to protect information provided to them in confidence.[39] Meanwhile, other provisions that protect confidential information are expressed to cover information the disclosure of which would constitute a breach of confidence.[40]

Personal information

3.36 A significant proportion of Commonwealth secrecy provisions—approximately one third—prohibit the disclosure of personal information. The majority of these provisions refer to information about a 'person'. As such, these provisions would also capture the disclosure of information about a body politic or corporate as well as a natural person.[41] However, some legislation refers to information relating to the affairs of an individual,[42] which refers to a natural person only.[43]

---

37 See, eg, *Water Act 2007* (Cth) s 215 (in which confidential information is not expressly defined); *Offshore Minerals Act 1994* (Cth) s 374 ('confidential information' is defined in a separate section, s 27).

38 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.

39 See, eg, *Water Act 2007* (Cth); *Australian Securities and Investments Commission Act 2001* (Cth) ss 213, 237; *Pooled Development Funds Act 1992* (Cth) s 71(5)(a) and (aa); *Bankruptcy Regulations 1996* (Cth) regs 8.05O, 8.32.

40 See, eg, *Industry Research and Development Act 1986* (Cth) s 47(1).

41 *Acts Interpretation Act 1901* (Cth) s 22.

42 See, eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 66; *Health Insurance Regulations 1975* (Cth) reg 23C(2)(a).

43 *Acts Interpretation Act 1901* (Cth) s 22.

3.37 Some secrecy provisions that protect information of this type use the term 'personal information',[44] which is the term used in the *Privacy Act 1988* (Cth) and the *Freedom of Information Act 1982* (Cth).[45] Other provisions refer to information 'about a person'[46] or 'concerning another person'.[47] The majority of secrecy provisions refer to information about the 'affairs' of another person.[48]

3.38 Secrecy provisions covering personal information are commonly found in contexts where individuals are required to provide information to government, such as taxation, health and social services, with the aim of protecting personal privacy.

3.39 Other secrecy laws that protect personal information prohibit the disclosure of information about the identity of particular persons, such as participants in witness protection programs,[49] officers of the Australian Security Intelligence Organisation (ASIO)[50] or people with assumed identities.[51] However, the purpose of secrecy provisions of this kind may extend beyond the protection of personal privacy to preventing other harms, for example, harm to national security or public safety.

Commercial information

3.40 Approximately 8% of secrecy provisions identified by the ALRC protect commercial information. Some of these provisions specify the type of confidential commercial information protected.[52] Other provisions protect commercial information by prohibiting disclosures that are likely to cause harm to commercial interests. 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.[53] While not expressly designated commercial information, secrecy provisions in legislation that regulate corporate entities, are likely to predominantly cover commercial information. For

---

44 See, eg, *Higher Education Support Act 2003* (Cth) ss 179-10, 179-35; *Product Grants and Benefits Administration Act 2000* (Cth) s 47(2); *Aged Care Act 1997* (Cth) s 86-2(1).

45 The *Privacy Act 1988* (Cth) and the *Freedom of Information Act 1982* (Cth) are discussed in Ch 16.

46 See, eg, *Superannuation Contributions Tax (Assessment and Collection) Act 1997* (Cth) s 32(1), (2); *Superannuation Guarantee (Administration) Act 1992* (Cth) s 45(1), (2).

47 See, eg, *Australian Institute of Health and Welfare Act 1987* (Cth) s 29(1).

48 See, eg, *Higher Education Funding Act 1988* (Cth) s 78(2); *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2); *Racial Discrimination Act 1975* (Cth) s 27F(1); *Health Insurance Act 1973* (Cth) s 130(1).

49 *Witness Protection Act 1994* (Cth) s 22.

50 *Australian Security Intelligence Organisation Act 1979* (Cth) s 92.

51 *Crimes Act 1914* (Cth) s 15XS.

52 See, eg, *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s 162; *Food Standards Australia New Zealand Act 1991* (Cth) s 114(1).

53 *Wheat Export Marketing Act 2008 (Cth)* s 73. See also *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth) s 22A (disclosure may cause substantial damage to a person's commercial or other interests); *Pooled Development Funds Act 1992 (Cth)* s 71(5)(b)(i) (disclosure may reasonably be expected to affect a person adversely in respect of the lawful business, commercial or financial affairs of the person); *Trade Practices Act 1974 (Cth)* s 95ZN (disclosure may damage the competitive position of the person).

example, secrecy provisions in the *Reserve Bank Act 1959* (Cth) protect information disclosed or obtained under, or for the purposes of the Act relating to the affairs of a financial institution; related body corporate or a person who has been, is, or proposes to be, a customer of a financial institution.[54]

Information relating to investigations

3.41 About 10% of secrecy provisions protect information which, if disclosed without authority, could prejudice the conduct of an investigation or inquiry. Such provisions are common in legislation relating to law enforcement, where secrecy provisions may prohibit the disclosure of information about the existence of a law enforcement operation or investigation;[55] the existence or content of a warrant,[56] summons or other notice or request,[57] or the questioning or detention of a person in certain circumstances.[58]

3.42 Secrecy provisions may also protect information obtained during or relating to investigations or inquiries outside of the law enforcement context. For example, secrecy provisions in the *Transport Safety Investigation Act 2003* (Cth) prohibit the unauthorised disclosure of 'restricted information', which is defined to include information obtained and recorded in the course of an investigation.[59] Some secrecy provisions also protect information obtained in the exercise of entry and search powers,[60] or given in evidence before a private hearing.[61]

3.43 Other secrecy provisions are framed to prohibit the disclosure of information that may prejudice an investigation. For example, s 35A of the *Ombudsman Act 1976* (Cth) prohibits the Ombudsman from disclosing information with respect to a particular investigation where the disclosure of that information is likely to interfere with the carrying out of any other investigation or the making of a report.

Other information

3.44 Specific secrecy provisions protect a variety of other, more particular kinds of information relevant to the context and function of particular legislative regimes, including information:

---

54 *Reserve Bank Act 1959* (Cth) s 79A. See also *Australian Prudential Regulation Authority Act 1998* (Cth) s 56.

55 See, eg, *Australian Crime Commission Act 2002* (Cth) s 29B (1), (3).

56 See, eg, *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS; *Telecommunications (Interception and Access) Act 1979* (Cth) ss 63, 133.

57 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 92; *Australian Crime Commission Act 2002* (Cth) s 29B(1); *Proceeds of Crime Act 2002* (Cth) ss 210, 217, 223; *Mutual Assistance in Criminal Matters Act 1987* (Cth) s 43C; *Crimes Act 1914* (Cth) s 3ZQT.

58 See, eg, *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS; *Criminal Code* (Cth) s 105.41.

59 *Transport Safety Investigation Act 2003* (Cth) ss 3, 60. See also, *Inspector of Transport Security Act 2006* (Cth) s 49; *Space Activities Act 1998* (Cth) s 96; *Civil Aviation Act 1988* (Cth) s 32AP.

60 See, eg, *National Environment Protection Measures (Implementation) Act 1998* (Cth) s 36.

61 See, eg, *Productivity Commission Act 1998* (Cth) s 53.

- of a specific type, such as cockpit voice recordings or on-board recordings[62] or the content or substance of a telegram;[63]
- provided as advice from particular committees and bodies;[64]
- derived from inspecting records;[65]
- comprising communications made during family counselling or dispute resolution;[66] and
- contained in applications, such as patent[67] or mining applications.[68]

3.45 Two specific kinds of 'other' information—defence and security information, and Indigenous cultural information—warrant more detailed explanation.

3.46 *Defence and security information*—a small number of specific secrecy provisions aim to prevent the unauthorised disclosure of defence or national security information.[69] Historically, the protection of this kind of information has been a core function of secrecy provisions. In addition to specific secrecy offences, defence and national security information is also protected by s 79 of the *Crimes Act* (disclosure of official secrets) and s 91.1 of the *Criminal Code* (Cth) (espionage).

3.47 Section 79 includes offences for the disclosure of information:

- made or obtained in contravention of pt VII of the *Crimes Act* (unlawful sounding) or s 91.1 of the *Criminal Code* (espionage);
- relating to a prohibited place or anything in a prohibited place that the person knows, or ought to know, should not be communicated.[70]

3.48 The most serious offence created by s 79 is the offence of communicating, retaining or receiving information with the intention of prejudicing the security or defence of the Commonwealth.[71]

---

62 *Civil Aviation Act 1988* (Cth) s 32AP; *Inspector of Transport Security Act 2006* (Cth) s 63; *Transport Safety Investigation Act 2003* (Cth) s 53.
63 *Postal and Telecommunications Commissions (Transitional Provisions) Act 1975* (Cth) s 37.
64 See, eg, *Environment Protection and Biodiversity Conservation Act 1999* (Cth) ss 189B, 251(3), 324R, 341R.
65 See, eg, *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) s 183-1; *Copyright Act 1968* (Cth) s 203E(10).
66 See, eg, *Family Law Act 1975* (Cth) ss 10D, 10H.
67 *Patents Act 1990* (Cth) s 173.
68 *Offshore Petroleum and Greenhouse Gas Storage Act 2006* (Cth) sch 5 cl 4.
69 See, eg, *Defence Force Discipline Act 1982* (Cth) s 58(1); *Defence Act 1903* (Cth) s 73A.
70 'Prohibited place' is defined in *Crimes Act 1914* (Cth) s 80 and includes defence property and installations.
71 Ibid s 79(2).

3.49 Section 91.1 of the *Criminal Code* 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[72] or give an advantage to another country's security or defence.[73]

3.50 In some secrecy 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'.[74]

3.51 *Indigenous sacred or sensitive information*—some 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[75] 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.[76]

Whose conduct is regulated?

3.52 The ALRC's mapping exercise shows that a range of different individuals and entities may be subject to secrecy provisions, including:

- Commonwealth employees;
- organisations or individuals providing services for or on behalf of the Commonwealth;
- Commonwealth agencies;

---

72 *Criminal Code* (Cth) s 91.1(3).
73 Ibid s 91.1(4).
74 See also *Auditor-General Act 1997* (Cth) s 37; *Patents Act 1990* (Cth) s 173; *Privacy Act 1988* (Cth) s 70; *Australian Human Rights Commission Act 1986* (Cth) s 24.
75 As defined in s 193S(1) of that Act.
76 See also *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3)(d).

- other specific categories of organisation or individual; and/or
- any person.

Commonwealth employees

3.53 Approximately one third of Commonwealth secrecy provisions apply to Commonwealth employees. In some cases, the provisions apply to all Commonwealth employees,[77] or all employees of the APS.[78]

3.54 Regulation 2.1 of the *Public Service Regulations* sets out the general duty of an APS employee not to disclose official information where it is reasonably foreseeable that the disclosure could prejudice the effective working of government. An APS employee is defined in s 7 of the *Public Service Act* to mean a person engaged by an agency head or by the Public Service Commissioner 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.[79]

3.55 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 and in Chapter 6.

3.56 Other secrecy provisions regulate officers in specific Commonwealth agencies, such as employees of Australia Post[80] or the staff of the Australian Human Rights Commission.[81] A small number of secrecy provisions apply to specific agency heads or officers—for example, the Commonwealth Ombudsman.[82]

Service providers to the Commonwealth

3.57 Some secrecy provisions expressly refer to a wider range of individuals than Commonwealth employees. This reflects changes to the structure of government and government service provision, and the view that information should be protected at every point in the 'distribution chain', including where that information is handled outside the public sector.[83]

---

77 See, eg, *Income Tax Assessment Act 1936* (Cth) s 16.
78 *Public Service Regulations 1999* (Cth) reg 2.1.
79 *Public Service Act 1999* (Cth) s 7.
80 *Australian Postal Corporation Act 1989* (Cth) ss 90H, 90LB apply to 'employees of Australia Post' by virtue of s 90G.
81 *Age Discrimination Act 2004* (Cth); *Disability Discrimination Act 1992* (Cth) s 127; *Sex Discrimination Act 1984* (Cth) s 112; *Racial Discrimination Act 1975* (Cth) s 27F.
82 *Ombudsman Act 1976* (Cth) s 35C.
83 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].

3.58 Around 10% of secrecy provisions expressly regulate consultants[84] and others who provide goods or services for or on behalf of the Australian Government.[85] In addition, service providers are often required by agencies to comply with confidentiality undertakings as part of service provision arrangements.[86]

Commonwealth agencies

3.59 About 10% of secrecy provisions apply to specific agencies or statutory corporations, as distinct from individuals.[87] The majority of provisions that apply to agencies are not criminal in nature, but are a component of a broader information-handling regime. For example:

- *Research Involving Human Embryos Act 2002* (Cth) s 29(4) requires the Licensing Committee to make certain information publicly available in a database; however, the database must not include 'confidential commercial information'.

- *Trade Practices Act 1974* (Cth) s 89(3) requires the Australian Competition and Consumer Commission (ACCC) to keep a register of applications for authorisations in respect of restrictive trade practices. Section 89(5A) requires that, where requested, the ACCC must keep certain information confidential, including information relating to 'secret formulas or processes' and the cost of manufacturing, producing or marketing goods and services.

- *Veterans' Entitlements Act 1986* (Cth) s 118ZF(7) provides that after determining a claim for a seniors health card, the Repatriation Commission must give the claimant a copy of its determination, except to the extent that the information is of a 'confidential nature' or might, if communicated, 'be prejudicial to the claimant's physical or mental health or well-being'.

3.60 Agencies are also subject to a range of other information-handling obligations, including under the *Privacy Act* and *Archives Act 1983* (Cth). These provisions are discussed further in Chapter 16.

---

84 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32(1).

85 See, eg, *Customs Administration Act 1985* (Cth) s 16.

86 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.

87 See, eg, *Australian Securities and Investments Commission Act 2001* (Cth) s 127(1) which applies to the Australian Securities and Investments Commission; and *Trade Practices Act 1974* (Cth) s 95ZP which applies to the Australian Competition and Consumer Commission.

Other organisations and individuals

3.61 Other secrecy provisions regulate a wide range of specific organisations and individuals, such as:

- state, territory or local government employees;[88]
- organisations and individuals who engage in federally funded or regulated areas of the private sector—for example, aged care providers;[89] and
- individuals assisting in government inquiries or studies.[90]

Any person

3.62 Around 30% of Commonwealth secrecy provisions are stated to apply to the handling of information by 'any person'. In the areas of criminal law enforcement and health and welfare, secrecy provisions that regulate the conduct of any person make up a high proportion (slightly less than half) of all secrecy provisions.

3.63 Secrecy provisions may be framed to regulate the conduct of any person where legislation provides a discretion to provide protected information to a potentially broad range of people. For example, s 135A(3) of the *National Health Act 1953* (Cth) permits the Secretary of the Department of Health and Ageing (DoHA) to disclose information to any person if the Minister certifies that disclosure to that person is necessary in the public interest. Section 135A(4) then applies the same secrecy obligations to any person who receives information pursuant to such a disclosure.

3.64 Secrecy provisions may also regulate the conduct of any person where the provision creates an ancillary offence such as soliciting, obtaining or offering to supply protected information.[91]

Current and former parties

3.65 Many secrecy provisions expressly regulate the behaviour of persons who hold, or have previously held positions through which they have access to Commonwealth information.

3.66 An example of a specific secrecy provision governing both current and former officers is s 191 of the *Aboriginal and Torres Strait Islander Act*, which expressly applies to a person:

---

88 See, eg, *Australian Hearing Services Act 1991* (Cth) s 67(8); *Taxation Administration Act 1953* (Cth) s 13J.

89 See, eg, *Aged Care Act 1997* (Cth) s 62-1.

90 See, eg, *Inspector of Transport Security Act 2006* (Cth) s 35(7); *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 4.

91 See, eg, *Social Security (Administration) Act 1999* (Cth) s 203; *Health Insurance Act 1973* (Cth) ss 130(14), 130(21); *Child Care Act 1972* (Cth) ss 12K, 12Q.

> (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.

3.67 The application of s 70 of the *Crimes Act,* which is expressed to apply to both current and former Commonwealth officers, may extend the application of other statutory secrecy provisions to former officers.

What conduct is regulated?

3.68 The vast majority (90%) of secrecy provisions prohibit the disclosure of Commonwealth information. Conduct such as tabling information in parliament, or serving information on other parties, may be regarded as forms of disclosure.

3.69 Secrecy provisions may also regulate other activities such as making a record (30%), using information (20%) or soliciting information (less than 5%).

3.70 The ALRC has identified a small number of secrecy provisions that regulate 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.[92] Two secrecy provisions apply to the mere receipt of information.[93]

3.71 Some secrecy provisions regulate both the initial and 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
>
> (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

---

92 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).

93 *Crimes Act 1914* (Cth) s 79(5), (6).

(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.

3.72 Other provisions make it an offence for a recipient of certain information then to use or disclose that information for other purposes. For example, under s 86-3 of the *Aged Care Act 1997* (Cth), the Secretary of DoHA may disclose protected information in certain circumstances, including where there is a risk to a person's 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.

Exceptions and defences

3.73 Most secrecy provisions contain 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 excuses conduct that is otherwise prohibited by a secrecy provision. An exception may provide, for example, that a Commonwealth officer does not commit an offence 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. The following discussion summarises exceptions and defences currently contained in secrecy laws.

3.74 Almost 20% of secrecy provisions do not contain any express exceptions or defences. 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 stated to be an offence of strict liability, the defence of mistake of fact remains available.[94]

Disclosure in the course of functions and duties

3.75 Approximately 35% of secrecy provisions allow information handling in the course or 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'.[95] Similar formulations appear in other areas of Commonwealth legislation.[96]

---

94 See *Criminal Code* (Cth) ss 6.1, 9.2.

95 *Taxation Administration Act 1953* (Cth) s 3C(2A).

96 See, eg, *Disability Services Act 1986* (Cth) s 28(2A); *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2); *Racial Discrimination Act 1975* (Cth) s 27F(3A).

Disclosure for the purposes of a particular law

3.76 Many secrecy provisions incorporate exceptions that allow the disclosure of information as required by a particular law. Secrecy provisions also commonly provide that information may be disclosed 'for the purposes of this Act'.[97] Some secrecy provisions also permit disclosure for the purposes of other legislation[98] or intergovernmental arrangements.[99]

Disclosure authorised by specified persons

3.77 Approximately 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'.[100]

3.78 Other secrecy provisions permit a specified person to authorise the handling of information—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;[101]

- 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;[102] 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.[103]

---

97 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).

98 See, eg, *Australian Human Rights Commission Act 1986* (Cth) s 49(3); *Reserve Bank Act 1959* (Cth) s 79A(2).

99 See, eg, *Disability Discrimination Act 1992* (Cth) s 127(3).

100 *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C(5)(b).

101 *Customs Administration Act 1985* (Cth) s 16(3).

102 *Health Insurance Act 1973* (Cth) s 130(3).

103 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 129(1).

Disclosure to specified persons or entities

3.79 Approximately 30% of secrecy provisions provide exceptions where disclosure is made to specified persons or entities. Often, the purpose of such exceptions is to authorise information sharing among Australian Government agencies. For example:

- the *Australian Prudential Regulation Authority Act 1998* (Cth) (APRA Act) permits the disclosure of information to the Australian Statistician, the Reserve Bank of Australia, auditors and actuaries;[104]

- the *Industry Research and Development Act 1986* (Cth) permits the disclosure of information to the Minister, ministerial staff, the Secretary of the Department or a designated officer of the Department;[105] and

- the *Gene Technology Act 2000* (Cth) permits the disclosure of information to 'the Commonwealth or a Commonwealth authority', a state agency, or the Gene Technology Technical Advisory Committee.[106]

3.80 In some instances, secrecy provisions permit disclosure in circumstances, or to persons or entities, as prescribed by regulation.[107]

Disclosure for the purposes of legal proceedings

3.81 Approximately 15% of secrecy provisions provide exceptions to expressly permit the disclosure of information for the purposes of court or tribunal proceedings.[108]

3.82 Some secrecy provisions provide that certain persons are not required to disclose information in court or tribunal processes, other than for the purposes of the Act under which the information was obtained.[109] 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.

Disclosure for the purposes of law enforcement

3.83 Approximately 15% of secrecy provisions include exceptions to allow the handling of information for various law enforcement and investigatory purposes. While

---

104 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(5A), (5B), (6A).
105 *Industry Research and Development Act 1986* (Cth) s 47(2).
106 *Gene Technology Act 2000* (Cth) s 187(1)(d).
107 See, eg, *Building and Construction Industry Improvement Act 2005* (Cth) s 65(4); *Medical Indemnity Act 2002* (Cth) s 77(4).
108 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).
109 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).

provisions of this kind often refer to the investigation of criminal offences,[110] some exceptions to secrecy provisions extend to broader law enforcement and administration of justice concerns. For example:

- 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 Commonwealth Ombudsman;[111]

- 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;[112] and

- the *Australian Federal Police Act 1979* (Cth) allows the Police 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'.[113]

Disclosure with consent

3.84 Approximately 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.[114] In addition, the *Privacy Act* contains exceptions to allow the use or disclosure of personal information with the person's consent.[115]

Disclosure of de-identified information

3.85 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.[116] For example:

- the APRA Act provides that it is not an offence if information is disclosed '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';[117] and

---

110 See, eg, *Surveillance Devices Act 2004* (Cth) s 45(5); *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(a).

111 *Crimes Act 1914* (Cth) s 23YO(2).

112 *Child Support (Assessment) Act 1989* (Cth) s 150(4D)–(4F).

113 *Australian Federal Police Act 1979* (Cth) s 60A(2B).

114 See, eg, *Gene Technology Act 2000* (Cth) s 187(1)(f); *Reserve Bank Act 1959* (Cth) s 79A(3); *National Health Act 1953* (Cth) s 135A(8).

115 *Privacy Act 1988* (Cth) s 14, IPPs 10, 11.

116 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].

117 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(7).

- 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'.[118]

Disclosure to avert threats to life or health

3.86 Some secrecy provisions contain exceptions permitting the disclosure of information in order to avert threats to a person's life or health, 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';[119]

- 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';[120] and

- the *Child Support (Assessment) Act* allows the disclosure of information to prevent or lessen a 'credible threat to the life, health or welfare of a person'.[121]

Disclosure in the public interest

3.87 A small number of secrecy provisions allow the disclosure of Commonwealth information in the public or national interest.

3.88 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'.[122] Similar provisions are found in other legislation.[123]

3.89 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'.[124]

General criminal offences

3.90 The remainder of this chapter examines the two general criminal offences in the *Crimes Act* relating to the unauthorised disclosure of Commonwealth information.

---

118 *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 11.
119 *Customs Administration Act 1985* (Cth) s 16(3F).
120 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34(1A).
121 *Child Support (Assessment) Act 1989* (Cth) s 150(3)(e).
122 *Food Standards Australia New Zealand Act 1991* (Cth) s 114(4).
123 See, eg, *Medical Indemnity Act 2002* (Cth) s 77(3); *Health Insurance Act 1973* (Cth) s 130(3); *National Health Act 1953* (Cth) s 135A(3).
124 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(b).

Section 70 covers the disclosure of information by Commonwealth officers, while s 79 deals with the disclosure of 'official secrets'. The following overview analyses each of these sections according to criteria similar to that used above to analyse specific secrecy provisions.

Section 70—disclosure of information by Commonwealth officers

3.91 Section 70 of the *Crimes Act* is the only provision remaining in pt VI of the *Crimes Act*.[125] 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).[126] 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.[127] While minor amendments have been made to s 70 on three occasions since 1960,[128] the substance of the provision has not changed since that time.

3.92 The effect of s 70 is to apply criminal sanctions to the breach of secrecy obligations by public officials.[129] Section 70 provides that:

> (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.

3.93 Many Australian states and territories have similar offences. Crimes legislation in Queensland, Western Australia, Tasmania, the Australian Capital Territory and the Northern Territory each contain broadly framed offences for the unauthorised disclosure of information by public officials.[130] All but the Northern Territory provision concern information that it is a person's duty to keep secret or not to disclose.[131] In New South Wales, the *Independent Commission Against Corruption Act*

---

125 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).

126 Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney-General), 265, 269. See also, J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 53.

127 *Crimes Act 1960* (Cth).

128 *Crimes Amendment Act 1982* (Cth); *Statute Law (Miscellaneous Provisions) Act 1987* (Cth); *Statute Law Revision Act 2008* (Cth).

129 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 214.

130 *Criminal Code* (Qld) s 85; *Criminal Code* (WA) s 81; *Criminal Code* (Tas) s 110; *Crimes Act 1900* (ACT) s 153; *Criminal Code Act 1983* (NT) s 76.

131 *Criminal Code Act 1983* (NT) s 76 refers to 'confidential information'.

1988 (NSW) includes as prohibited 'corrupt conduct' the 'misuse of information or material that [a public official] has acquired in the course of his or her official functions, whether or not for his or her benefit or for the benefit of any person'.[132]

3.94 Since 2000, the majority of prosecutions for the breach of secrecy provisions have been brought under s 70 of the *Crimes Act*, even where specific secrecy offences would have been available. There have been successful prosecutions for breaches of s 70, including of:

- an officer of the Australian Taxation Office—for providing documents containing summaries of taxpayers and tax agents to a private business associate;[133]
- an officer of the Australian Customs Service—for providing reports about security at Sydney Airport to journalists;[134]
- an officer of the Office of Indigenous Policy Coordination—for disclosing information relating to the then draft *Declaration on the Rights of Indigenous Peoples*[135] to her daughter, and information relating to Commonwealth Indigenous policy to a member of the Mutitjulu community in the Northern Territory;[136] and
- 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.[137]

3.95 The following section examines the terms of s 70 of the *Crimes Act* in more detail.

'Duty not to disclose'

3.96 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 in a specific secrecy provision.[138] In *R v Goreng Goreng*, for example, the duty was found in reg 2.1(3) of the *Public Service Regulations*, which provides that APS employees must not disclose information obtained or generated in connection with their

---

132 *Independent Commission Against Corruption Act 1988* (NSW) s 8(1)(d). South Australia has only a general provision relating to improper conduct by public officials: *Criminal Law Consolidation Act 1935* (SA) s 238.
133 *R v Petroulias (No 36)* [2008] NSWSC 626.
134 *R v Kessing* (2008) 73 NSWLR 22; *Kessing v The Queen* [2008] NSWCCA 310.
135 *Declaration on the Rights of Indigenous Peoples*, G.A. Res. 61/295,U.N. Doc. A/RES/47/1 (2007).
136 *R v Goreng Goreng* [2008] ACTSC 74.
137 Transcript of Proceedings, *R v Sweeney*, (District Court Queensland, Shanahan J, 28 March 2001).
138 See, eg, *R v Goreng Goreng* [2008] ACTSC 74, [8].

employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government.

3.97 Although the issue has not been determined by a court, 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 with loyalty 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'.

3.98 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.[139] However, in *Director of Public Prosecutions v G,* the Full Court of the Federal Court considered 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'.[140] The Court was not, however, required to determine this issue.

3.99 Under s 70, criminal sanctions apply 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 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).[141] 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.[142]

What kind of information is protected?

3.100 Section 70 of the *Crimes Act* 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.

3.101 In *Commissioner of Taxation v Swiss Aluminium Australia Ltd*, Bowen CJ of the Federal Court commented that:

---

139 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 259.

140 *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.

141 *Cortis v R* [1978] WAR 30, 32. See also J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 52–53.

142 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 259.

> 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.[143]

3.102 Higgins J of the Supreme Court of the ACT 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.[144]

3.103 The application of s 70 to the disclosure of information will depend on the nature of the duty not to disclose. As noted above, for example, the equitable duty of confidentiality only arises where the disclosure would be inimical to the public interest.[145] Therefore, a prosecution for an offence under s 70, reliant on a breach of an equitable 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 obtained in the course of employment, s 70 could potentially apply to the disclosure of information already in the public domain.[146]

3.104 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.[147]

3.105 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

---

143 *Commissioner of Taxation v Swiss Aluminium Australia Ltd* (1986) 10 FCR 321, 325.
144 *Deacon v Australian Capital Territory* [2001] ACTSC 8, [87]–[88].
145 *Commonwealth v Fairfax* (1980) 147 CLR 39.
146 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 216.
147 Ibid, 212–213.

airport security arrangements to two journalists.[148] 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.[149]

3.106 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.[150]

What kind of activity is regulated?

3.107 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 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.[151]

3.108 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.[152]

---

148 *Walworth v Merit Protection Commissioner and Another* [2007] FMCA 24. A summary of this case appears in Ch 2.

149 *Kessing v The Queen* [2008] NSWCCA 310, [61].

150 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 261.

151 *Kessing v The Queen* [2008] NSWCCA 310, [31].

152 Ibid, [36].

Whose activity is regulated?

3.109 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, Australian Defence Force, Australian Federal Police or public authority under the Commonwealth;
- who performs services for or on behalf of the Commonwealth, a territory or public authority; or
- who performs services, or is an employee of the Australian Postal Corporation.

3.110 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,[153] ministers and ministerial staff all potentially fall within the definition.[154] 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.[155]

3.111 Other legislation may deem certain officers to be Commonwealth officers. For example, officers or employees of ASIO[156] and staff members of the Australian Secret Intelligence Service[157] are deemed to be Commonwealth officers for the purposes of the *Crimes Act.*

Exception—authorised disclosures

3.112 Section 70(1) includes an exception to the offence where a 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 by requiring that the publication or communication be 'without lawful authority or excuse', proof of which lies with the defendant.

---

153 See comments by Gummow J in *Grollo v Palmer* (1995) 184 CLR 348, 396.

154 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'.

155 Issues relating to the application of secrecy provisions to judicial officers are discussed in Ch 6.

156 *Australian Security Intelligence Organisation Act 1979* (Cth) s 91.

157 *Intelligence Services Act 2001* (Cth) s 38.

3.113 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 clarify 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 of a Commonwealth officer may provide an implied authority to release information.[158] 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.[159]

3.114 Section 70 does not create an exception or defence relating to disclosure in the public interest. However, it is possible that this issue might be a factor in sentencing in a particular case.[160]

Section 79—disclosure of official secrets

3.115 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).[161] While s 79 deals with the disclosure of defence or security information, there is also significant overlap with the general secrecy offence in s 70. Section 79 is set out in full in Appendix 5.

3.116 By way of background, the *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth) 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.[162]

158 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 261.

159 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 259.

160 See, eg, comments by Bennett SC DJC in *Walworth v Merit Protection Commissioner and Another* [2007] FMCA 24, [49]–[63].

161 Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney-General), 265.

162 Criminal Code Amendment (Espionage and Related Offences) Bill 2001 (Cth) cl 82.4.

3.117 The new provisions were criticised on the basis that they would interfere with freedom of speech and prevent public discussion of important issues of public interest.[163] 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.[164]

3.118 There have been few prosecutions under s 79. One example is the conviction in 2003 of Simon Lappas for offences under ss 79(3) and 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, Sherryll Dowling, so she could sell the documents to a foreign country.[165] 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.[166]

3.119 Another example is the conviction in 1977 of a probationary trainee of ASIO for 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.[167]

What kind of information is protected?

3.120 Section 79 operates as both a general and a specific secrecy provision, depending on the kind of information disclosed. As noted above, s 79(1)(a) and (c) set

---

163 R Sharman, 'Espionage and Related Offences Bill' (2002) 21(1) *Communications Law Bulletin* 7, 8.

164 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.

165 *R v Lappas* (2003) 152 ACTR 7.

166 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.

167 *Grant v Headland* (1977) 17 ACTR 29.

out two categories dealing with the disclosure of particular kinds of defence and security information. However, s 79 also covers a more general category of 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;
>
> (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.[168]

3.121 Section 79(1)(b) is similar to that in s 70, insofar as it 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 dependent on 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 of a particular security classification—or the circumstances in which the information was obtained.

3.122 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'.[169]

What kind of activity is regulated?

3.123 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:

- Section 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.

168 *Crimes Act 1914* (Cth) s 79(1)(b).
169 Ibid s 77(1).

- Section 79(3): communicating or allowing someone to have access to an official secret without authorisation—maximum penalty two years imprisonment.

- Section 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.

- Section 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.

- Section 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.

3.124 Apart from s 79(2), which requires that a person act intending to prejudice the security or defence of the Commonwealth, s 79 applies to all information, regardless of its nature or the effect of its disclosure. As noted in 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.[170]

Whose activity is regulated?

3.125 Section 79 covers the unauthorised disclosure of information obtained and generated by Commonwealth officers and information 'entrusted' to other persons by Commonwealth officers. The offence therefore covers both initial disclosures by Commonwealth officers and subsequent disclosures by third parties. In addition, the offences relating to the receipt and handling of an official secret apply to any person, regardless of whether the person was aware that he or she had a duty not to disclose information.[171]

Exceptions and defences

3.126 Subsections 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.

---

170 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 242.
171 *Grant v Headland* (1977) 17 ACTR 29, 31.

3.127 The exception regarding a duty to communicate information 'in the interest 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*.[172] Clive 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 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*.

3.128 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.[173]

3.129 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*,[174] which set out factors relevant to determining the public interest in the confidentiality and disclosure of certain information.[175]

3.130 Subsections 79(5) and (6) include a defence to the offence of receiving prescribed information where a person can prove that the 'communication was contrary to his or her desire'.

Overlap between the general offences

3.131 There is a degree of overlap between ss 70 and 79(3) of the *Crimes Act.* The offence under s 79(3), 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)).

3.132 While both offences apply to Commonwealth officers who disclose information without authority, s 79(3) extends to subsequent disclosure of information by 'any person'. Further, s 79(4), (5) and (6) applies to conduct other than disclosure, including the unauthorised retention or receipt of information.

---

172 *R v Ponting* [1985] Crim LR 318.
173 Ibid. The jury found Ponting not guilty.
174 *Commonwealth v Fairfax* (1980) 147 CLR 39.
175 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 266.

3.133 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.[176]

3.134 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 potential for uncertainty about the kind of conduct that will attract criminal sanctions.

3.135 The following chapters set out a framework for the reform of general and specific secrecy provisions in Commonwealth legislation to provide greater certainty and to ensure a consistent and workable approach to the protection of Commonwealth information.

176 Ibid.

4. Framework for Reform

Contents

Introduction

4.1 In Chapter 3, the ALRC discusses 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. In this chapter the ALRC considers whether these general law obligations provide sufficient protection in the public sector context, and whether it is necessary and desirable also to have in place statutory provisions that impose obligations of confidentiality on Commonwealth officers and others who handle Commonwealth information. The chapter then examines the potential role of administrative, civil and criminal provisions in regulating the disclosure of Commonwealth information.

4.2 The ALRC's key recommendation for reform in the criminal context is that, in most cases, 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 an essential public interest, the ALRC has formed the 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.[1]

The need for statutory secrecy provisions

4.3 In Chapter 2, the ALRC considers the role of secrecy in the context of modern trends to more open and accountable government, including the development of freedom of information (FOI) laws, and the need to share government information more widely across government and with the private sector. In this section, the ALRC considers whether statutory secrecy provisions still have a legitimate role to play in protecting Commonwealth information.

Submissions and consultations

4.4 In the course of this Inquiry, there was sustained support for the principle of open access to government information. For example, the Law Council of Australia commented that:

> the principle of open and accountable government, which underpins the [*Freedom of Information Act 1982* (Cth) (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.[2]

4.5 To similar effect, the Media, Entertainment and Arts Alliance 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 [Australian Labor Party] identified a 'culture of concealment' which had grown up within the government and public service and promised to 'drive a cultural shift across the bureaucracy to promote a pro-disclosure culture'. The Alliance supports this objective which we believe to be greatly in the public interest.[3]

4.6 However, stakeholders also recognised the need to protect government information in some circumstances. The Australia's Right to Know (ARTK) coalition argued that, while access to government information is 'an essential right' of every Australian and 'fundamental to openness, transparency and accountability in government', access could be restricted in certain limited circumstances:

> 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

---

1 Administrative penalties and contractual remedies are considered in detail in Chs 12–14.
2 Law Council of Australia, *Submission SR 30,* 27 February 2009.
3 Media Entertainment & Arts Alliance, *Submission SR 39,* 10 March 2009.

> bureaucratic considerations that persist in much of the current legislation should not be relevant considerations.[4]

4.7 While the Australian Government Attorney-General's Department (AGD) acknowledged that 'openness 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'.[5]

4.8 The Australian Securities and Investments Commission (ASIC) noted that a high proportion of the information it receives and develops is confidential. It considered that unauthorised disclosure of such information has the potential to impact adversely on both public and private interests, including the effective functioning of the Australian economy as well as the effective functioning of ASIC such as the conduct of investigations. Such disclosures might also impact on the free and frank exchange of information with government, regulated entities and foreign regulators.[6]

4.9 ASIC emphasised that 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.[7]

4.10 A number of other agencies also highlighted the importance of secrecy provisions with respect to their particular operations. For example, the Australian Bureau of Statistics (ABS) considered that secrecy laws are necessary 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.[8]

4.11 The ABS noted that this assurance is based on an 'unwritten compact' between the ABS and census respondents that their personal information will be protected. This compact is underwritten by the secrecy provisions in the ABS governing legislation.[9]

---

4 Australia's Right to Know, *Submission SR 35,* 6 March 2009.
5 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
6 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.
7 Ibid.
8 Australian Bureau of Statistics, *Submission SR 28,* 24 March 2009.
9 Ibid.

4.12 Other federal bodies also emphasised the importance of secrecy provisions in areas that deal with personal information. The Australian Taxation Office (ATO), for example, 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'.[10] The expectations of the Australian community in relation to the handling of personal information were also emphasised by the Department of Employment, Education and Workplace Relations (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.[11]

4.13 Both the Treasury and the ATO submitted that taxation secrecy provisions were 'not inconsistent' with measures 'designed to increase the openness and transparency of government', including FOI laws. The Treasury stated that taxation secrecy provisions are not designed to conceal the deliberations of government but to give effect to the legitimate expectations of Australia's taxpayers that the sensitive personal information they are required to provide will be appropriately protected.[12]

4.14 The Department of Human Services (DHS) drew attention to the broad role that secrecy provisions 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.[13]

4.15 Information in the hands of intelligence agencies was also seen to require the protection of secrecy provisions. The Australian Intelligence Community (AIC)

---

10 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

11 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.

12 The Treasury, *Submission SR 22,* 19 February 2009; Australian Taxation Office, *Submission SR 13,* 16 February 2009.

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

submitted that 'a statutory duty on Commonwealth officers not to disclose information is fundamental to the operation of AIC agencies'.[14]

4.16 The Australian Transaction Reports and Analysis Centre (AUSTRAC) reiterated the relevance and necessity of secrecy provisions to prevent the 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 Transaction Reports Act 1988* (Cth)], or who are reporting entities or dealers under those Acts.[15]

4.17 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)], 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.[16]

ALRC's views

4.18 In Chapter 3, the ALRC discusses the application of the general law to the protection of Commonwealth information—including the common law duty of loyalty and fidelity owed by employees and the equitable duty of confidence. The chapter highlights the difficulties and uncertainties that have arisen in applying these legal principles—developed in the private sector—to the protection of information in the public sector.

4.19 The recommendations in this Report are aimed at providing a conceptual framework for the protection of information in the Australian Government public sector that takes account of the various public interests that do not operate to the same degree in the private sector—including, for example, the need for openness and accountability, the requirement to release information under FOI laws, and the shift to a pro-disclosure culture in government. The ALRC recognises that a balance must be found between the principles of open government and the need to protect

---

14 Australian Intelligence Community, *Submission SR 37,* 6 March 2009. The AIC agencies are the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Defence Intelligence Organisation, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate, and the Office of National Assessments.

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

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

Commonwealth information where unauthorised disclosure would harm identified public interests.

4.20 The problems identified throughout this Inquiry have not been in relation to the existence of secrecy provisions, as such, but rather in relation to the scope and number of provisions, and the lack of clarity in particular provisions. The ALRC's view is that there is a legitimate need for statutory secrecy provisions regulating the handling of Commonwealth information, provided that they are clear and consistent, and directed at protecting important public interests. In the following section, the ALRC considers whether such protection is best achieved by relying on the criminal or civil law, or through the use of administrative provisions and penalties.

Criminal, civil or administrative provisions

4.21 As discussed in Chapter 3, statutory provisions that impose secrecy obligations carry a range of administrative, civil or criminal penalties. Of the 506 secrecy provisions identified by the ALRC, approximately 70% impose criminal penalties.[17] While the remaining provisions do not expressly contain criminal penalties, some establish a duty not to disclose Commonwealth information and have the potential to attract the penalties imposed by s 70 of the *Crimes Act 1914* (Cth).[18]

4.22 A number of secrecy provisions allow the imposition of administrative sanctions on Australian Government employees—such as termination of employment, a reduction in salary or a reprimand. 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 Chapter 12, 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'.[19]

4.23 Finally, the ALRC has identified one secrecy provision in the *Environment Protection and Biodiversity Conservation Act 1998* (Cth) that imposes civil penalties.[20]

4.24 Regulatory theory cautions against the over-use of criminal penalties. Criminal penalties sit at the top of the 'enforcement pyramid' developed by Professors Ian Ayres

---

17 See Appendix 4.

18 Section 70 of the *Crimes Act* and the need to establish an external 'duty not to disclose' are discussed below.

19 *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 *Parliamentary Service Act 1999* (Cth) s 13(6) read with s 15; and the *Cadet Force Regulations 1977* (Cth) sch 4 cl 5 read with ss 16 and 17.

20 *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 170B.

and John Braithwaite to describe a model regulatory approach.[21] 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.[22]

4.25 Although this model was developed for the corporate regulatory environment, the principles of the enforcement pyramid model are broadly applicable to the issues under consideration in this Inquiry. At the bottom of the enforcement pyramid lie the techniques described in Chapters 14 and 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.

4.26 In the following section, the ALRC considers the role of administrative, civil and criminal penalty provisions in protecting Commonwealth information.

Administrative provisions

4.27 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 only be imposed by courts.[23] Commonwealth employees will often be subject to secrecy obligations, breach of which may result in the imposition of administrative penalties by an agency head.

---

21 The model was first put forward by Braithwaite in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985). See also I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (1992).

22 Quoted in F Haines, *Corporate Regulations: Beyond 'Punish or Persuade'* (1997), 218–219.

23 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.

4.28 For example, as considered in detail in Chapter 12, where an APS employee breaches the APS Code of Conduct, 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;[24] or a reprimand.[25] While some of these penalties—such as termination of employment—are quite severe, they are considered disciplinary rather than criminal in nature.

4.29 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.

4.30 Soon after the Public Service Bill 1997 (Cth)[26] 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.[27]

4.31 Administrative penalties under the *Public Service Act*, and other similar legislation,[28] 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.

Submissions and consultations

4.32 In the Issues Paper, *Review of Secrecy Laws* (IP 34), the ALRC asked whether there were any breaches of secrecy provisions that should only give rise to administrative penalties. [29] Stakeholders suggested that administrative penalties may

---

24 *Public Service Act 1999* (Cth) s 15; *Public Service Regulations 1999* (Cth) reg 2.3.

25 *Public Service Act 1999* (Cth) s 15.

26 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].

27 P Shergold, 'A New Public Service Act: The End of the Westminster Tradition?' (1997) 85 *Canberra Bulletin of Public Administration* 32, 34.

28 Such as the *Parliamentary Service Act 1999* (Cth); *Defence Force Discipline Act 1982* (Cth); *Australian Federal Police Act 1979* (Cth); *Cadet Force Regulations 1977* (Cth).

29 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–13.

be preferable to criminal proceedings for relatively minor breaches,[30] or where the harm caused by the breach was likely to be relatively low.[31] Dr Ian Turnbull suggested that administrative penalties would 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.[32] Liberty Victoria was of the view that administrative penalties should be used where there was no intentional or reckless behaviour.[33]

ALRC's views

4.33 In Chapter 12, the ALRC considers in detail the role of secrecy provisions that impose administrative penalties on public sector employees. In the ALRC's view such provisions have a central 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 relatively minor. Administrative penalties provide a range of responses to different levels of misconduct. They allow misconduct 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.

4.34 Further, by addressing obligations associated with employment in the public sector, administrative secrecy provisions may also protect different interests from those recognised in the criminal context. This will include, for example, 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'.[34]

4.35 In Chapters 12 and 13, 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 13, the ALRC also makes a number of recommendations 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.

---

30 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.

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

32 I Turnbull, *Submission SR 15,* 17 February 2009.

33 Liberty Victoria, *Submission SR 19,* 18 February 2009. ASIC submitted that administrative penalties would be appropriate where an unauthorised disclosure is inadvertent: Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.

34 *Public Service Act 1999* (Cth) s 3.

Civil penalty provisions

4.36 As noted above, the ALRC has identified only one secrecy provision that imposes a civil penalty—s 170B of the *Environment Protection and Biodiversity Conservation Act.* This provision 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.[35]

4.37 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.[36]

4.38 Most civil penalties are monetary. Civil penalty provisions may also provide for the imposition of compensation orders[37] or community service orders.[38] 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.

4.39 The AGD *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (*Guide to Framing Commonwealth Offences*) 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).[39]

4.40 Taking into account recommendations made by the ALRC in its report on civil and administrative penalties,[40] 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:

- where criminal punishment is not warranted—contraventions of the law involving serious moral culpability should only be pursued by criminal prosecution;

---

35 The maximum pecuniary penalty for breach of this provision is 100 penalty units (currently $11,000).

36 See Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 62.

37 See, eg, *Corporations Act 2001* (Cth) ss 1317H, 1317HA; *Trade Practices Act 1974* (Cth) s 87.

38 See, eg, *Trade Practices Act 1974* (Cth) s 86C.

39 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 63.

40 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002).

- 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.[41]

4.41 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).[42] Another example, of more direct relevance to this Inquiry, is s 25 of the *Commonwealth Authorities and Companies Act 1997* (Cth)—which imposes civil penalties on officers and employees of Commonwealth authorities governed by the Act 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.

4.42 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.[43]

Submissions and consultations

4.43 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.[44] The ATO also expressed the view that the unauthorised handling of taxpayer information should be subject to criminal penalties:

> 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

---

41 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 63–64.

42 *Corporations Act 2001* (Cth) pt 9.4B.

43 A Freiberg, 'Civilizing Crime: Reactions to Illegality in the Modern State' (1985) *Thesis*, 120.

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

> having civil options available for breach of a tax secrecy provision, as well as Code of Conduct action under the *Public Service Act*.[45]

4.44 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.[46] 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.[47]

4.45 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.[48]

4.46 Dr 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.[49]

4.47 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 difficult to assess and quantify the damage to the integrity of the Cabinet process caused by disclosure of a Cabinet document'.[50]

---

45 Australian Taxation Office, *Submission SR 13,* 16 February 2009.
46 Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.
47 Liberty Victoria, *Submission SR 19,* 18 February 2009.
48 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009.
49 J Renwick, *Submission SR 02,* 11 December 2008.
50 Attorney-General's Department, *Submission SR 36,* 6 March 2009.

ALRC's views

4.48 As noted above, the ALRC has identified only one civil penalty provision among the hundreds of secrecy provisions considered in this Inquiry.[51] 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.

4.49 The ALRC has considered the existing civil penalty provision 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.

4.50 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC asked 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 and, if so, whether there is a role for civil penalty provisions in addressing this gap.[52] The limited response from stakeholders on this question seemed to indicate that there were no significant problems in this area. Accordingly, the ALRC is not making any recommendations that would give civil penalties a greater role in relation to the protection of Commonwealth information.

4.51 In addition, in Chapter 7, the ALRC recommends that the courts be given an express power to issue injunctions to restrain a breach of the general secrecy offence or the on-disclosure of information in breach of the subsequent disclosure offences.[53] This recommendation recognises that preventing the disclosure of sensitive Commonwealth information is preferable to imposing sanctions once disclosure has occurred.

---

51 *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 170B.

52 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Question 14–1.

53 Recommendation 7–6. The subsequent disclosure offences regulate the disclosure of Commonwealth information by any person where the information has been disclosed by a Commonwealth officer in breach of the general secrecy offence or on terms requiring that the information be held in confidence.

Criminal provisions

4.52 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.[54]

4.53 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 2006 Treasury *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions*.[55] 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.[56]

4.54 A number of submissions to this Inquiry also emphasised the importance of the deterrent value of criminal penalties.[57]

4.55 In considering whether a criminal penalty is appropriate in relation to particular conduct, regard must be had to the effect of a criminal conviction; 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.

---

54 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.

55 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 15.

56 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].

57 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.

Effect of a criminal conviction

4.56 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'.[58]

4.57 A conviction is a judicial act that alters an offender's legal status.[59] 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.[60] A conviction has many consequences beyond the immediate penalty imposed. A person who is convicted of certain offences may be:

- ineligible to hold public office;[61]
- ineligible to manage a corporation,[62] or be a director or principal executive officer of a company;[63]
- 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;[64] and
- deported, if he or she is a non-citizen.[65]

4.58 A convicted offender may lose, 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.

4.59 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*

---

58 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 11.

59 R Fox and A Freiberg, 'Sentences Without Conviction: From Status to Contract in Sentencing' (1989) 13 *Criminal Law Journal* 297, 300.

60 See, eg, Human Rights and Equal Opportunity Commission, *Discrimination in Employment on the Basis of Criminal Record—Discussion Paper* (2004).

61 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).

62 *Corporations Act 2001* (Cth) s 206B.

63 See, eg, *Life Insurance Act 1995* (Cth) s 245.

64 This is subject to the spent conviction provisions in *Crimes Act 1914* (Cth) pt VIIC.

65 *Migration Act 1958* (Cth) s 201.

(Cth), which establishes a scheme to trace, restrain and confiscate the proceeds of crime committed against federal law.

Conduct deserving of criminal sanctions

4.60 A number of commentators and reports have considered the circumstances in which it is appropriate for criminal sanctions 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.

4.61 John McGinness has questioned the need for criminal penalties to protect much of the information currently covered by secrecy provisions. He suggested that a large number of secrecy provisions could be repealed, and reliance placed instead 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 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*).[66]

4.62 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'.[67]

4.63 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

66 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 76.

67 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.

> reserved for serious offences where the public interest is best served by imposing those sanctions on the offender.[68]

Submissions and consultations

4.64 In IP 34, the ALRC asked when the 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.[69]

4.65 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 of 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.[70]

4.66 The AIC 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.[71]

4.67 APRA noted that the deterrent value of criminal penalties is important where there is much to gain by disclosing commercial information.[72] The Australian Commission for Law Enforcement Integrity also commented on the importance of the deterrence value of criminal penalties.[73]

4.68 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'.[74] 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

---

68 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].

69 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–1.

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

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

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

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

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

> not provide a remedy that is most appropriate for the particular circumstances of each breach.[75]

4.69 The 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 (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.[76]

4.70 DEEWR 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 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.[77]

4.71 Other stakeholders noted that criminal penalties should only be used when strictly required for the effective functioning of government. 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.[78]

4.72 Whistleblowers Australia stated that, while criminal penalties may be appropriate in relation to the unauthorised disclosure of information that is likely to harm the public interest, the processes of government should generally only be protected by administrative sanctions.[79]

---

75 Ibid.
76 Department of Human Services, *Submission SR 26,* 20 February 2009.
77 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.
78 Liberty Victoria, *Submission SR 19,* 18 February 2009. See also Law Council of Australia, *Submission SR 30,* 27 February 2009.
79 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.

4.73 The APS Commissioner agreed that not all unauthorised disclosures should attract criminal penalties, in light of the administrative penalty regime in place in relation to APS employees. The Commissioner noted, however, that:

> it is important to retain the link to criminal penalties, as there is merit in the general deterrent value of a criminal offence.
>
> … I believe that the system preventing unauthorised disclosure of Commonwealth information needs to be clearly articulated and simple to apply on a practical level. Whatever criminal offence is devised to replace section 70 should be simple, easy to understand, and reflect the proper balance between open, accountable government and effective public administration.[80]

4.74 PIAC noted that the unauthorised disclosure of confidential non-government information in the private sector gives rise—in the absence of personal dishonesty such as fraud or insider trading—to civil liability only, but noted that 'disclosure by a government employee of innocuous government information can currently give rise to criminal liability'.[81] The ARTK coalition expressed the view that criminal penalties should only apply where there is an overwhelming public interest in preventing disclosure; and the consequences of disclosure adversely affect national security, law enforcement or public safety.[82]

4.75 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.[83]

ALRC's views

4.76 The ALRC considers 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'.[84] It seems clear, however, that there is a legitimate role for the criminal law in certain circumstances. Commonwealth information includes a range of highly sensitive information, such as national security information and information relating to defence and law enforcement. Unauthorised disclosure of this kind of information has

---

80 Australian Public Service Commission, *Submission SR 56,* 7 August 2009.
81 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009.
82 Australia's Right to Know, *Submission SR 72,* 17 August 2009.
83 R Fraser, *Submission SR 42,* 23 March 2009.
84 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].

the capacity to cause real harm to important public interests, and to the effective functioning of government.

4.77 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 essential 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.

General and specific secrecy offences

4.78 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.[85]

4.79 Although s 79 is generally concerned with the disclosure of defence or security information, 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 persons owing to their position as current or former Commonwealth officers that, by reason of its nature or the circumstances under which the information was made or obtained, or for any other reason, it is their duty to treat as secret.

4.80 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'.[86]

4.81 In addition to the general secrecy offences in ss 70 and 79(3) of the *Crimes Act*, the ALRC has identified numerous specific secrecy offences in other legislation.[87]

ALRC's views

4.82 The ALRC considers that there is a need for a general secrecy offence, to be included in the *Criminal Code* (Cth), for the following reasons. The general offence is intended to replace s 70 of the *Crimes Act* and to serve as an umbrella offence applying to all current and former Commonwealth officers and all Commonwealth information. The general offence would cover gaps left by specific secrecy provisions that focus, for example, on a particular function of an agency or on particular information held by an agency.

---

85 These offences are described in detail in Ch 3 and set out in full in Appendix 5.

86 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [35.12].

87 A list of all secrecy provisions identified by the ALRC is set out in Appendix 4.

4.83 The ALRC is not suggesting, however, that the general offence replace all existing secrecy offences. In Chapter 8, the ALRC recommends that specific secrecy offences should only be put in place or retained where they differ in significant and justifiable ways from the general offence.[88] Chapters 8 to 11 consider the circumstances in which specific secrecy provisions imposing criminal sanctions remain justified.

4.84 In Chapter 6, the ALRC also recommends two subsequent disclosure offences.[89] These offences would regulate disclosure by any person who received Commonwealth information in breach of the general secrecy offence or on terms requiring it to be held in confidence. The subsequent disclosure offences, in combination with the general secrecy offence, are intended to replace s 79(3) of the *Crimes Act.*

4.85 Finally, the repeal of s 70 of the *Crimes Act* will give rise to the need to consider those specific secrecy provisions that give rise to a 'duty not to disclose' for the purposes of s 70. There are a number of options available in relation to these provisions, for example, it would be possible to leave the provisions in place as information-handling provisions that do not attract criminal sanctions.[90] Alternatively, if the circumstances justify criminal sanctions, the provisions may need to be amended to create separate criminal offences.

A harm-based approach

Duty not to disclose information

4.86 In considering how these new secrecy offences should be framed, the ALRC examined a range of existing provisions—including ss 70 and 79(3) of the *Crimes Act*—particularly 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 of the *Crimes Act*.

4.87 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 3, 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.

88 Recommendation 8–3.
89 Recommendations 6–6, 6–7.
90 This issue is discussed in Ch 10.

4.88 For example, s 13 of the *Public Service Act*, which sets out the APS Code of Conduct, provides that an APS employee must comply with any conduct requirement prescribed by the regulations.[91] 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 foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.[92]

4.89 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.

4.90 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.

4.91 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.[93] The ALRC has also identified 23 provisions that are not themselves criminal, but may give rise to a 'duty not to disclose' for the purposes of s 70.[94]

4.92 A duty may also arise from other sources, such as an employee's general law duties[95] or, possibly, the terms and conditions of an employment contract. As discussed in Chapter 3, there is some doubt about whether the 'duty' in s 70 of the *Crimes Act* can arise from a contractual term, but it seems clear that it must be a legal—as opposed

---

91 *Public Service Act 1999* (Cth) s 13(13).

92 The full text of reg 2.1 of the *Public Service Regulations* is set out in Appendix 5.

93 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.

94 As explained in Ch 3, s 70 of the *Crimes Act* makes it an offence for a Commonwealth officer to disclose information which it is his or her duty not to disclose. These provisions are included in Appendix 4 and marked with an asterisk.

95 The common law duty of loyalty and fidelity and the equitable duty of confidence are considered in Ch 3.

to a moral—duty.[96] The lack of clarity as to which 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.[97]

4.93 In his report on *Integrity in Government Project—Official Information*, Paul Finn expressed the view that the operation of s 70

> 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.[98]

4.94 The AGD *Guide to Framing Commonwealth Offences* 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.[99]

4.95 In DP 74, the ALRC expressed the view that it was not desirable for the scope of a central element of the general secrecy offence to be dependent on provisions in other legislation.[100] This approach leaves open the possibility that a single criminal penalty, set out in s 70, will apply to a wide range of circumstances set out in specific secrecy provisions. Although it is possible 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 expressed concern that, where no cross-reference to s 70 was included in legislation containing a duty of non-disclosure, it was unclear whether the Australian Parliament expressly considered the link with s 70 and the fact that a breach of the duty created had the potential to give rise to criminal liability and the imposition of the criminal sanctions set out in s 70.

---

96 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 258–259.

97 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 73.

98 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 43–44.

99 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 14.

100 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Ch 7.

Submissions and consultations

4.96 In response to IP 34, the 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.[101]

4.97 Other stakeholders expressed a level of concern that the duty not to disclose should be found separately from the provision imposing the criminal sanction.[102] The Community and Public Sector Union (CPSU) focused on the relationship between reg 2.1 of the *Public Service Regulations* and s 70 of the *Crimes Act* and 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.[103]

4.98 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.[104]

4.99 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.[105]

ALRC's views

4.100 There are real concerns about the way that s 70 of the *Crimes Act* is framed—in particular, the need to establish a 'duty not to disclose' independently of the offence provision. In the ALRC's view, where it is the Australian Parliament's intention to

---

101 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
102 See, eg, Law Council of Australia, *Submission SR 30,* 27 February 2009.
103 Community and Public Sector Union, *Submission SR 32,* 2 March 2009.
104 R Fraser, *Submission SR 42,* 23 March 2009.
105 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009.

impose criminal sanctions for disclosure of Commonwealth information, this should be done in a single offence provision so that there is a clear and certain link between the conduct being criminalised and the criminal penalty imposed.

4.101 In addition, it is not appropriate to impose criminal sanctions for breach of any duty not to disclose Commonwealth information. In the ALRC's view, for example, the duties defined by an employee's duty of loyalty and fidelity or those set out in reg 2.1 of the *Public Service Regulations* are too broad to form the basis of a criminal offence.[106]

Alternative approaches

4.102 In this section, the ALRC considers alternative approaches to framing secrecy offences and concludes that the duty not to disclose information should be set out in the provision itself, and that it should be framed as a duty not to disclose information that would harm, or is likely or intended to harm, essential public interests. This approach has the potential to address the issues identified above: that is, it will not be necessary to look to other legislation to define the duty not to disclose, and it will be possible to ensure that criminal penalties are only imposed in appropriate circumstances by identifying the public interests to be protected by each offence.

Past reports and recommendations

4.103 A number of past reports in Australia and overseas have considered various ways of framing secrecy provisions, including by defining protected categories of information or adopting a harm-based approach. In 1972, a United Kingdom (UK) departmental committee chaired by Lord Franks (the Franks Committee), reported on s 2 of the *Official Secrets Act 1911* (UK).[107] Section 2 prohibited the unauthorised disclosure of 'all information which a Crown servant learns in the course of his duty'.[108] The Committee noted that:

> The leading characteristic of this offence is its catch-all quality. It catches all official documents and information. It makes no distinctions of kind, and no distinctions of degree. All information which a Crown servant learns in the course of his duty is 'official' for the purposes of section 2, whatever its nature, whatever its importance, whatever its original source. A blanket is thrown over everything; nothing escapes. The section catches all Crown servants as well as all official information.[109]

106 Regulation 2.1 is discussed in Ch 12, including a number of recommendations for reform.
107 Departmental Committee on Section 2 of the *Official Secrets Act 1911*, *Report of the Committee*, Vol 1 (1972).
108 Ibid, 14.
109 Ibid.

4.104 The Franks Committee concluded that 'any law which impinges on the freedom of information in a democracy should be much more tightly drawn'.[110] The Committee concluded that change was essential, and that s 2 should be repealed and replaced by narrower and more specific provisions.[111] The Committee rejected 'the notion that criminal sanctions should be retained for all official information which a Government may reasonably wish to withhold' and, in particular, expressed the view that information about most of the domestic functions of government should not attract the protection of the criminal law.[112] This approach was intended to minimise the inhibiting effect of s 2 on the appropriate disclosure of information about these functions.

4.105 Instead, the Franks Committee concluded that only information that went to the fundamentals of government, and that had the potential to affect the nation as a whole and the safety of its citizens, should attract the protection of the criminal law:

> A safe and independent life for a nation and its people requires effective defence against the threat of attack from outside. It requires the maintenance of the nation's relations with the rest of the world, and of its essential economic base. It requires the preservation of law and order, and the ability to cope with emergencies threatening the essentials of life … It is information relating to these basic functions of a central Government which most requires protection. It is here that a threat to the nation can have the most serious consequences. The most appropriate general description for all these matters is that they concern the security of the nation and the safety of the people.[113]

4.106 The Franks Committee identified the following kinds of official information as requiring the protection of the criminal law:

- classified information relating to defence or internal security, or to foreign relations, or to the currency or to the reserves, the unauthorised disclosure of which would cause serious injury to the interests of the nation;
- information likely to assist criminal activities or to impede law enforcement;
- Cabinet documents; and
- information entrusted to the Government by a private individual or organisation.[114]

4.107 In relation to the first category, the Franks Committee recommended that the existing security classification system be adapted, so that information classified at

110 Ibid, 37.
111 Ibid, 40.
112 Ibid, 43.
113 Ibid, 46.
114 Ibid, 101.

'Secret' and above would attract the protection of the criminal law.[115] The prosecution would be required to establish that the information was classified, but not that the disclosure of the information would harm the interests of the nation.[116] In relation to the second category, the prosecution would have to prove that the information was likely to assist criminal activities or impede law enforcement, thus imposing a requirement to prove that the disclosure was likely to cause harm. Cabinet documents and information provided by individuals or organisations were to be protected as categories of information and the prosecution would not be required to prove harm.

4.108 The Committee stated, in relation to repealing and replacing s 2 of the *Official Secrets Act*:

> We propose its replacement by provisions reduced in scope and less uncertain in operation. We believe that these provisions provide the necessary minimum of criminal law required for the security of the nation and the safety of the people, and for the constructive operation of our democracy in the conditions which obtain today.[117]

4.109 A 1978 UK Government Home Office White Paper[118] set out proposals for legislation that closely followed the Franks Committee's recommendations, but legislation introduced in 1979 based on this White Paper was withdrawn due to lack of support. A second Home Office White Paper was published in 1988, taking a different approach. The 1988 White Paper proposed that the legislation should

> identify those areas in which disclosure of at least some information may be sufficiently harmful to the public interest to justify the application of criminal sanctions. The number of such areas is in fact small. For the most part, even if disclosure may obstruct sensible and equitable administration, cause local damage to individuals or groups or result in political embarrassment, it does not impinge on any wider public interest to a degree which would justify applying criminal sanctions.[119]

4.110 In addition, the 1988 White Paper proposed that various tests of harm should be developed:

> The Government considers that as far as possible any test of harm should be concrete and specific if it is to be applied by the courts. At this practical level, the harm likely to arise from the disclosure of different kinds of information is not the same in all respects in each case. The Government therefore proposes separate tests of likely harm for the different categories of information to be covered by future legislation.[120]

---

115 The Australian Government security classification scheme is discussed in Ch 14.

116 Departmental Committee on Section 2 of the *Official Secrets Act 1911*, *Report of the Committee*, Vol 1 (1972), 56.

117 Ibid, 12.

118 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1978).

119 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [24].

120 Ibid, [22].

4.111 The White Paper proposed that the legislation should apply in the areas of:

- security and intelligence;
- defence;
- international relations;
- information obtained in confidence from other governments and international organisations;
- information useful to criminals; and
- interception information.

4.112 The White Paper proposed a harm element in relation to each of these areas except disclosures of security and intelligence information by members of the security and intelligence services; information obtained in confidence from other governments and interception information. The *Official Secrets Act 1989* (UK) was based to a large extent on the approach outlined in this White Paper and is discussed further below.

4.113 The UK developments were considered in Australia by the Gibbs Committee. In its final report, the committee discussed the need for secrecy offences in Australia 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 dealing with 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, [the provisions] 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.[121]

4.114 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; or
- obtained in confidence from foreign governments and international organisations.[122]

---

121 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 322.

122 Ibid, 331. 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: 332.

4.115 In some areas, however, 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.[123]

4.116 In the 2004 report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, the ALRC recommended that criminal penalties should be imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.[124] As discussed in Chapter 3, this is the approach that the courts have adopted in considering the extent to which government information is protected by the equitable duty of confidence.[125]

Australian secrecy offences

4.117 Most existing secrecy provisions in Australia do not expressly indicate the public interest they are seeking to protect or the harm they are seeking to prevent. 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.

4.118 This provision binds the Chief Executive Officer, staff and others associated with the Australian Crime Commission, 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. While this issue 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,[126] or by the court in deciding on an appropriate penalty,[127] they do not form an element of the offence itself.

---

123 Ibid, 323. This issue is discussed further in relation to specific secrecy offences in Ch 8.

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

125 *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd* (1987) 10 NSWLR 86; *Commonwealth v Fairfax* (1980) 147 CLR 39.

126 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* (2009), [2.10].

127 Section 16A(2)(e) of the *Crimes Act 1914* (Cth) provides that the court must have regard to any injury, loss or damage resulting from the offence.

4.119 By way of contrast, a small number of Australian secrecy provisions expressly require that the unauthorised conduct cause, be likely to cause, or be intended to cause, harm to a specific public interest.[128] An example is s 58 of the *Defence Force Discipline Act 1982* (Cth), which provides that it is an offence to make an unauthorised disclosure of information that 'is 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.

4.120 Another example is s 193S(3) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth), which makes it an offence for an Indigenous Land Corporation 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'.

4.121 As noted above, and discussed in Chapters 2 and 12, reg 2.1(3) of the *Public Service Regulations* was amended in 2006 to incorporate a harm element. The revised regulation prohibits an APS employee from disclosing Commonwealth information 'if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government'. Although this provision does not itself give rise to criminal sanctions, it does establish a 'duty not to disclose' that can be used as the basis for a criminal prosecution under s 70 of the *Crimes Act.*

4.122 The requirement to establish that the unauthorised disclosure could be prejudicial to the effective working of government was introduced following a decision of the Federal Court of Australia in *Bennett v President, Human Rights and Equal Opportunity Commission*.[129] Finn J found that reg 7(13)—a predecessor to reg 2.1—was a 'catch-all' provision that did not differentiate between the types of information protected or the consequences of disclosure and was therefore inconsistent with the implied constitutional freedom of communication about government and political matters.[130]

4.123 The constitutional validity of the amended reg 2.1 was challenged in the Supreme Court of the ACT in *R v Goreng Goreng* (*Goreng Goreng*).[131] The regulation was upheld on the basis that it was much more limited than its predecessor and targeted the protection of a legitimate public interest in the effective working of government.[132]

---

128 A number of these specific secrecy provisions are discussed in more detail in Ch 8.

129 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

130 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'.

131 *R v Goreng Goreng* [2008] ACTSC 74.

132 Ibid, [37].

Case study: *R v Goreng Goreng*[133]

Tjanara Goreng Goreng was a Commonwealth officer with the Office of Indigenous Policy Co-ordination in the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA). Goreng Goreng was charged with seven counts of breaching a duty not to disclose information which came into her possession in her capacity as a Commonwealth officer. Goreng Goreng sent her daughter three documents relating to the rights of Indigenous peoples, to assist her with an essay she was writing for school. Goreng Goreng also forwarded a number of work related emails—having removed the 'confidential' marking on one email—to the payroll/finance officer in the community administration at the Mutitjulu community.

The jury found Goreng Goreng guilty of a breach s 70 of the *Crimes Act*. The prosecution argued that the 'duty not to disclose' under s 70 was activated by the duty set out in reg 2.1 of the *Public Service Regulations*; the common law duty of an employee to serve her employer in good faith and fidelity; the equitable duty of confidence imposed on recipients of confidential information; and the obligation under s 13(10) of the *Public Service Regulations* not to use information for personal benefit.

Goreng Goreng was convicted and released upon entering into a recognizance in the sum of $2,000 to remain of good behaviour for three years and to pay a penalty in the sum of $2,000 within six months.

International secrecy offences

4.124 The *Official Secrets Act 1989* (UK), the *Crimes Act 1961* (NZ) and the *Summary Offences Act 1981* (NZ) have each adopted a harm-based approach to the disclosure of certain categories of official information.

4.125 The UK *Official Secrets Act* requires the prosecution to prove that an unauthorised disclosure of information in the following categories is 'damaging':

- security and intelligence information disclosed by Crown servants and government contractors;
- defence;

133 Ibid.

- international relations; and
- criminal law enforcement.

4.126 As discussed further below, there is no requirement under the Act to prove harm in relation to disclosures of security and intelligence information by members of the security and intelligence services; telecommunications interception information; and information obtained under a warrant issued under the *Security Services Act 1989* (UK).

4.127 Section 78A of the New Zealand *Crimes Act* establishes an offence for unauthorised communication of official information 'likely to prejudice the security or defence of New Zealand'. In addition, s 20A of the *Summary Offences Act 1981* (NZ) establishes an offence for unauthorised communication of official information likely:

> (a) to endanger the safety of any person; or
>
> (b) to prejudice the maintenance of confidential sources of information in relation to the prevention, investigation, or detection of offences; or
>
> (c) to prejudice the effectiveness of operational plans for the prevention, investigation, or detection of offences or the maintenance of public order, either generally or in a particular case; or
>
> (d) to prejudice the safeguarding of life or property in a disaster or emergency; or
>
> (e) to prejudice the safe custody of offenders or of persons charged with offences; or
>
> (f) to damage seriously the economy of New Zealand by disclosing prematurely decisions to change or continue Government economic or financial policies relating to:
>
> (i) exchange rates or the control of overseas exchange transactions;
>
> (ii) the regulation of banking or credit;
>
> (iii) taxation;
>
> (iv) the stability, control, and adjustment of prices of goods and services, rents, and other costs, and rates of wages, salaries, and other incomes;
>
> (v) the borrowing of money by the Government of New Zealand;
>
> (vi) the entering into of overseas trade agreements.

4.128 All of these offences in the New Zealand *Crimes Act* and *Summary Offences Act* require the prosecution to prove harm.

Discussion Paper proposal

4.129 In DP 74, the ALRC considered the need to reduce significantly the scope of s 70 of the *Crimes Act*.[134] The ALRC suggested that this could be achieved in a number of ways. One option would be to target the unauthorised disclosure of specific categories of information—for example, information relating to national security or defence; classified information; information provided in confidence by other governments or international organisations; or Cabinet documents.

4.130 The ALRC did not, however, adopt this approach, expressing the view that—in relation to the general secrecy offence—it was important to ensure that only disclosures of information that genuinely required protection, and which were likely to be harmful, should attract criminal sanctions. Not all information in any one of the categories above would meet this test. Instead, the ALRC proposed that the new general secrecy offence should apply to unauthorised disclosures of Commonwealth information that were reasonably likely to, intended to, or did in fact:

- harm the national security, defence or international relations of the Commonwealth;
- 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;
- endanger the life or physical safety of any person;
- pose a serious threat to public health or public safety;
- have a substantial adverse effect on personal privacy; or
- 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.[135]

Submissions and consultations

In support of an express harm requirement

4.131 A number of stakeholders expressed support for the ALRC's proposed approach of imposing criminal sanctions under the general secrecy offence in relation to

134 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Ch 6.
135 Ibid, Proposal 7–1. Each of these public interests is discussed in detail in Ch 5 of this Report.

unauthorised disclosures that cause harm, or are likely or intended to cause harm, rather than simply relying on protected categories of information.[136] The CPSU, for example, considered that the approach 'provides an appropriate balance between secrecy, and transparency and openness of government' and that the proposed provision was a 'significant improvement upon s 70 of the *Crimes Act* in providing clarity and consistency for regulating secrecy of government information'.[137]

4.132 PIAC had previously 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 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 has the decided advantage of leaving open an exception where disclosure would expose serious wrongdoing or iniquity.[138]

4.133 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) (FOI Act), which is 'limited only by exceptions and exemptions necessary for the protection of essential public interests and the private and business affairs of persons'.[139]

4.134 The Law Council of Australia also noted this tension, stating that it is anomalous that criminal sanctions may be imposed on a public servant for releasing 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, stating 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.[140]

---

136 R Fraser, *Submission SR 78,* 21 August 2009; L McNamara, *Submission SR 51,* 6 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

137 Community and Public Sector Union, *Submission SR 57,* 7 August 2009.

138 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.

139 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009. The relationship between secrecy provisions and freedom of information is considered in Ch 16.

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

4.135 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:

> 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.[141]

4.136 The AGD noted that this approach had been taken in reg 2.1 of the *Public Service Regulations*, discussed above. 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, however, 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)'.[142] 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. [143]

4.137 AUSTRAC also expressed support for the proposed general secrecy offence, noting that it captured those public interests that should be afforded protection by the criminal law. AUSTRAC submitted, however, that a different approach is required in relation to the general secrecy offence and specific secrecy offences:

> AUSTRAC considers that to extend the specific secrecy offences to 'all information' which a Commonwealth officer has, or had, access to by reason of being a Commonwealth officer, is too broad in the context of the discussion of harm in regard to specified public interests. The current secrecy provisions of the [*Anti Money Laundering and Counter-Terrorism*] *Act* and [*Financial Transaction Reports*] *Act* protect a sub-set of information on the basis that its disclosure may adversely impact national security, international relations and the prevention, detection, prosecution and punishment of criminal offences, the recovery of criminal assets and protection of the national revenue.[144]

4.138 ASIC submitted that criminal liability should be limited to unauthorised disclosures of information that genuinely requires protection and that is likely to harm

---

141 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
142 Ibid.
143 Ibid.
144 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

a public or private interest, but emphasised that, if a harm element were introduced, the provisions should be explicit about the public interests they are intended to protect.[145]

4.139 The ARTK coalition acknowledged that criminal sanctions are likely to be justified in circumstances where unauthorised disclosure of information causes or is reasonably likely to cause:

- harm to national security, defence or international relations;
- prejudice to law enforcement activities or the protection of the public revenue;
- danger to the life or physical safety of any person; or
- a serious threat to public health or safety.[146]

4.140 While supporting the proposed focus on the harm caused by unauthorised disclosures, the ARTK coalition suggested that the offence should also be limited to defined categories of information, as suggested by the Gibbs Committee.[147]

4.141 The Australian Press Council acknowledged that certain government information needed to be kept confidential, but expressed the view that 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.[148]

4.142 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.[149]

Concerns raised in relation to an express harm requirement

4.143 A number of stakeholders were concerned that the introduction of an express harm requirement would lead to a lack of clarity and certainty for Commonwealth

145 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.
146 Australia's Right to Know, *Submission SR 72,* 17 August 2009.
147 Ibid.
148 Australian Press Council, *Submission SR 16,* 18 February 2009.
149 Whistleblowers Australia, *Submission SR 40,* 10 March 2009.

officers and other stakeholders.[150] The Department of Immigration and Citizenship, for example, stated that:

> There may be a degree of subjectivity in assessing whether the disclosure of information would cause harm to a specified public interest, which could be difficult to apply in practice. For example, assessing potential harm caused by unlawful disclosure of information about asylum seekers will be subjective and difficult to measure given sensitive issues such as removal and possible impact on family members in country of origin.[151]

4.144 FaHCSIA noted that the test may be difficult to apply in practice, and especially difficult to prove beyond reasonable doubt. FaHCSIA expressed support for s 70 of the *Crimes Act*, noting that the strength of the provision lay in its broad application. The Department referred to the successful prosecution in *Goreng Goreng*,[152] expressing the view that criminal sanctions were appropriate in that case, and noting that it would have been difficult to achieve the same result under the proposed new general secrecy offence.[153]

4.145 FaHCSIA acknowledged, however, that there may be merit in improving the clarity and certainty of s 70, in particular by clarifying how the 'duty not to disclose' might arise:

> This could be done, for example, by codifying the core elements of the 'duty not to disclose' in subsection 13(10) of the *Public Service Act 1999*, regulation 2.1 of the *Public Service Regulations 1999*, and the common law duty of an employee to serve in good faith and fidelity.[154]

4.146 The CDPP echoed FaHCSIA's concerns in relation to prosecuting the proposed new general secrecy offence and, in particular, the requirement to prove harm:

> the issue would be one for the trier of fact (ie a jury on indictable matters). Specific evidence would need to be lead on the harm (or likely harm) to the public interest. It would then be open to a defendant to rebut the prosecution case by arguing the disclosure did not (or was not reasonably likely to) cause harm to the public interest.[155]

4.147 The CDPP argued that the discussion in open court of whether a disclosure of sensitive Commonwealth information caused, or was reasonably likely, or intended to cause, harm to the public interest did not seem consistent with the protection of that

---

150 Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; The Treasury, *Submission SR 22,* 19 February 2009.

151 Department of Immigration and Citizenship, *Submission SR 59,* 7 August 2009.

152 *R v Goreng Goreng* [2008] ACTSC 74.

153 Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.

154 Ibid.

155 Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009.

public interest. In the national security context, for example, the CDPP stated that the act of giving evidence about such matters would be likely to further prejudice the public interest.

4.148 The CDPP was also concerned about who would be able to give evidence of harm, or the likelihood of harm—for example, ministers or senior Commonwealth officials—and what sort of evidence would be necessary to prove the matters beyond reasonable doubt. The CDPP noted that it is likely that the views of ministers or senior government officers would be considered opinion evidence, and that opinion evidence is only admissible when it is given by persons who fall within the various categories of 'experts' recognised in the *Evidence Act 1995* (Cth).[156]

4.149 The Australian Federal Police stated that it opposed the requirement to prove harm in all cases in light of the difficulty of discharging the evidential burden:

> For certain types of information the harm caused by disclosure will be apparent, for example, the release of police intelligence to the targets of an investigation. However, there will be large grey areas where showing the harm from disclosure will be complex, for example, the release of the architectural plans of a Commonwealth government building. Proving beyond reasonable doubt to a court that the release of such plans is likely to cause harm may require the production of evidence showing the agency and activities carried on in the building, the motivations of the person receiving the information and the context of its release. While it may be easy to argue intellectually that a disclosure caused, or is likely to cause, harm, quantifying the harm in court through admissible evidence may be difficult.[157]

4.150 APRA and the 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.[158] 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.[159]

---

156 Section 79(1) of the *Evidence Act 1995* (Cth) provides: 'If a person has specialised knowledge based on the person's training, study or experience, the opinion rule does not apply to evidence of an opinion of that person that is wholly or substantially based on that knowledge'.

157 Australian Federal Police, *Submission SR 70,* 14 August 2009.

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

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

ALRC's views

The need for reform

4.151 Despite the views of some stakeholders that s 70 of the *Crimes Act* is relatively straightforward to enforce and should be retained, the 'catch-all' nature of the provision is seriously out of step with public policy developments in Australia and internationally. As discussed in Chapter 2, there is also an argument to be made that a law that imposes criminal liability on all Commonwealth officers for unauthorised disclosure of any official information—and does not differentiate between the types of information protected or the consequences of disclosure—does not sit comfortably with the implied constitutional freedom of communication about government and political matters, or with Australia's international human rights obligations.[160]

4.152 An attempt to codify or define the 'duty not to disclose', as suggested by one stakeholder, is unlikely to avoid the problem of having to establish that a disclosure had the potential to cause harm. An employee's duty of loyalty and fidelity, for example, requires that an employee must not use or disclose information obtained in the course of his or her employment to the detriment of the employer.[161] Regulation 2.1 requires that APS employees must not disclose information that could be prejudicial to the effective working of government.

4.153 The ALRC has identified two ways in which the general secrecy offence could be framed. First, the offence could identify categories of information that require protection. For example, a number of stakeholders suggested that various categories of information—such as Cabinet documents and information supplied in confidence by a foreign government—should be protected by the general secrecy offence. If this approach were adopted, it would not be necessary to prove that a disclosure caused harm, but rather that the information disclosed fell within the protected category.

4.154 Alternatively, the offence could be structured so that only those unauthorised disclosures that caused harm, or were reasonably likely or intended to cause harm, would attract criminal sanctions.

Categories of information

4.155 The weakness of the 'categories of information' approach is that it is indiscriminate. While the choice of category may reflect a sense that disclosure of any information in the category would inherently or potentially cause harm, the emphasis is not on the harm, but on the category. The ALRC is not convinced that all the

---

160 In particular art 19 of the *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976).

161 The duty of loyalty and fidelity is discussed in Ch 3.

information in the categories suggested would cause harm if disclosed, or warrants the protection of the criminal law.[162]

4.156 The alternative approach, recommended by the ALRC, is that the new general secrecy offence should expressly identify the harms that the provision seeks to prevent.[163]

The harm-based approach

4.157 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, to an essential public interest. This approach balances the need to protect certain Commonwealth information with the public interest in an open and accountable system of government. It also means that the sanctions of the criminal law are reserved for the more serious cases of unauthorised disclosure.

4.158 The ALRC acknowledges, however, that in some limited circumstances, 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, making an express requirement to prove the harm unnecessary. In these circumstances, it may be appropriate to frame the secrecy offence in relation to a particular category of information. This issue is discussed in relation to specific secrecy offences in Chapter 8.

4.159 It is not possible to adopt this approach in the general secrecy offence, however, because it is intended to apply to all Commonwealth officers and all Commonwealth information. In these circumstances, the harm to the public interest that would be caused by an unauthorised disclosure is not implicit. The unauthorised disclosure of any Commonwealth information should not be sufficient of itself to found a criminal offence, particularly in light of the Australian Government policy of encouraging a pro-disclosure culture in the public sector, and the fact that harm is unlikely to arise in relation to much of the information held by government.

Concerns with the harm based approach

4.160 A number of stakeholders expressed concern that an offence including a harm element would be difficult for Commonwealth officers to apply in practice. While there is scope for the exercise of an officer's judgement in deciding whether the disclosure of certain Commonwealth information would, for example, damage national security, defence or international relations, the ALRC is not convinced that this will make the provision unworkable. The Australian Public Service Commission has noted

---

162 Each of these suggested categories of information is discussed in Ch 5.
163 Recommendation 5–1.

that APS employees are already required to consider on each occasion whether the disclosure of information could damage the effective working of government.[164]

4.161 However, most disclosures will be routine and cause no harm. If the disclosure occurs in the course of an officer's functions and duties, for example, it is expressly excluded from the general secrecy offence.[165] If a Commonwealth officer is unsure whether a certain disclosure is likely to cause harm, then a certain amount of consideration and consultation would be appropriate. In most agencies, this situation is likely to arise only rarely, if ever. It may be that the issue can be resolved at officer level but, if not, disclosures made with the authority of the agency head or the minister are also expressly excluded from the general offence.[166]

4.162 The ALRC has considered stakeholder concerns that a requirement to prove harm would give rise to evidential difficulties. The CDPP, for example, noted that it is likely to require the use of 'opinion evidence' as to the harm or the reasonable likelihood of harm. Section 76 of the *Evidence Act 1995* (Cth) sets out the 'opinion rule', and provides that evidence of an opinion is not admissible to prove the existence of a fact. There are a number of exceptions to this rule, however, including s 79 of the Act, which provides that the 'opinion rule' does not apply where a person has specialised knowledge based on the person's training, study or experience, and the person's opinion evidence is wholly or substantially based on that knowledge.

4.163 As discussed in the report, *Uniform Evidence Law* (ALRC 102), there is not a clear distinction between factual evidence and opinion evidence, but rather there exists a continuum with evidence of a purely factual nature at one end and evidence that is essentially someone's opinion at the other.[167] This would be true of the harm elements that the ALRC is recommending should form part of the general secrecy offence. In some cases the harm will be a matter of fact, for example, where an unauthorised disclosure compromises a criminal investigation because it alerts suspects to the investigation and gives them the opportunity to evade arrest; or where an unauthorised disclosure of a person's contact details results in threatening behaviour towards that person. At the other end of the continuum will be cases where the harm will have to be proved by the use of expert opinion evidence, for example, where it is alleged that the unauthorised disclosure was reasonably likely to harm international relations.

---

164 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009.

165 Recommendation 7–1(a).

166 Recommendation 7–1(b).

167 Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [9.3].

4.164 Section 79 of the *Evidence Act* provides scope for senior Commonwealth officers with relevant training or experience to be called to give evidence of harm or likely harm in areas such as national security, defence, international relations, or public safety. The ALRC notes that under s 60A of the FOI Act—amended by the *Freedom Information (Removal of Conclusive Certificates and Other Measures) Act 2009* (Cth)—the Inspector-General of Intelligence and Security may be asked to appear before the Administrative Appeals Tribunal to give evidence on the damage that would, or could reasonably be expected to, be caused to the security, defence or international relations of the Commonwealth by the release of a document. This provision recognises that the Inspector-General does have relevant specialised knowledge in these areas.

4.165 The CDPP also expressed concern that proving harm in open court might require the introduction of evidence that would further harm the public interest. In some cases, this issue will simply not arise, for example, where the information and context is already in the public domain because of the disclosure, or where the need for secrecy has passed due to the passage of time.

4.166 Where there is a need to introduce sensitive information into evidence, courts have developed processes and rules to deal with the situation—including the closing of courts and the use of suppression orders to restrict publication of proceedings and access to court files. These processes are discussed in detail in the ALRC report, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98).[168] The ALRC also notes that the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) establishes procedures to protect information likely to prejudice national security from disclosure in federal criminal proceedings.[169]

Specific secrecy offences

4.167 In Chapter 8 the ALRC expresses the view that specific secrecy offences prohibiting the disclosure of information obtained or generated by intelligence agencies—without the need to prove harm in every case—are justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies. The ALRC also states that in some very limited cases, and where the category of information protected is narrowly defined, certain agencies—such as the ATO, Centrelink and the ABS, as well as some corporate regulators—may also be able to justify specific secrecy offences that do not include an express harm requirement. Generally, however, the ALRC recommends that specific secrecy offences should include an express requirement that the unauthorised

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

169 The *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) was enacted following a report by the ALRC on protecting national security information during court proceedings: Ibid. The Act deals only with certain aspects of federal criminal and civil proceedings, however, and does not canvass the broader range of issues considered by the ALRC.

disclosure of information caused, or was likely or intended to cause, harm to an essential public interest.[170]

Conclusion

4.168 For these reasons the ALRC considers that most secrecy offences, and the general secrecy offence in particular, should include an express requirement to establish that an unauthorised disclosure of Commonwealth information caused, or was likely or intended to cause, harm to specified public interests. This approach balances the need to protect some information by means of the criminal law, with the public interest in open government and the fostering of a pro-disclosure culture in the Australian public sector.

Recommendation 4–1 Sections 70 and 79(3) of the *Crimes Act 1914* (Cth) should be repealed and replaced by new offences in the *Criminal Code* (Cth)—the 'general secrecy offence' and the 'subsequent disclosure offences'.

170 Recommendation 8–2.

5. General Secrecy Offence: Harm to Public Interests

Contents

Introduction

5.1 In Chapter 4, the ALRC recommends that s 70 of the *Crimes Act 1914* (Cth) be repealed and that there should be a new general secrecy offence located in the *Criminal Code* (Cth).[1] The ALRC also concludes that most secrecy provisions, and the general secrecy offence in particular, should include an express requirement to establish that an unauthorised disclosure of Commonwealth information caused, or was likely or intended to cause, harm to specified public interests. In this chapter the ALRC considers which specific public interests should be protected by the general offence. In developing its approach to this issue, the ALRC took as its starting point the exceptions set out in the *Freedom of Information Act 1982* (Cth) (FOI Act).

5.2 In formulating a provision to target the protection of specific public interests, the ALRC was drawn to the idea that the general secrecy offence 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 of the *Public Service Regulations 1999*

1 Recommendation 4–1. Section 70 is described in detail in Chs 3 and 4, and set out in full in Appendix 5.

(Cth), which prohibits the disclosure of information that has the potential to prejudice the effective working of government.[2] 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.[3]

5.3 The ALRC has adopted the approach that a subset of the public interests identified in the FOI Act exemptions should inform the development of the public interests to be protected by the general secrecy offence. This approach has the additional benefit that FOI guidelines and jurisprudence in relation to the meaning and scope of these FOI exemptions may assist Commonwealth officers to better understand their obligations under the new general secrecy offence.

5.4 In the course of the Inquiry a number of stakeholders expressed views on the ALRC's general approach to this issue and the range of public interests that should be expressly protected by the general secrecy offence. The Australian Securities and Investments Commission (ASIC) agreed that secrecy provisions and FOI legislation should be complementary and that 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 secrecy provisions with the need to release information into the public domain under the FOI Act.[4]

5.5 The Australian Government Attorney-General's Department (AGD) noted the ALRC's preference for moving away from the protection of categories of information in the general secrecy offence, but expressed the view that some limited categories of information did merit protection on the basis that the information had the potential to harm 'processes or relationships that are an integral part of government'.[5]

5.6 The Australia's Right to Know (ARTK) coalition advocated

> 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.[6]

---

2 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009.

3 *Freedom of Information Act 1982* (Cth) s 3(1)(b). The Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) proposes a revised objects clause, which is set out in Ch 2 of this Report.

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

5 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

6 Australia's Right to Know, *Submission SR 35,* 6 March 2009.

5.7 The Law Council of Australia expressed the view that the 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.[7]

5.8 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC proposed that the general secrecy offence should impose criminal penalties for the unauthorised disclosure of information that did, 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.[8]

5.9 In the following section, the ALRC considers in detail the FOI exemptions that should be reflected in the general secrecy offence.

What should be included in the general secrecy offence?

Damaging national security, defence or international relations

5.10 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, defence or international relations of the Commonwealth.[9]

---

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

8 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 7–1.

9 *Freedom of Information (Removal of Conclusive Certificates and Other Measures) Act 2009* (Cth) sch 1 cl 5 repeals the provisions of the FOI Act that previously permitted a minister or delegate to issue a conclusive certificate in relation to documents exempt under s 33(1) of the FOI Act.

National security and defence

5.11 In this section the ALRC considers whether unauthorised disclosures that damage the security or defence of the Commonwealth should be covered by the general secrecy offence.

5.12 As discussed in Chapter 4, the departmental committee on s 2 of the *Official Secrets Act 1911* (UK) chaired by Lord Franks (Franks Committee) recommended that, in the United Kingdom (UK), information relating to internal security or defence and classified 'Secret' or above should be protected by criminal secrecy offences. This was on the basis that such information was classified because unauthorised disclosure would cause 'at least serious injury to the interests of the nation'.[10]

5.13 The Committee noted that the criterion for classification would have to be applied correctly and consistently if the system were to operate fairly. It recommended that, before making a decision to prosecute for the unauthorised disclosure of any classified information, the responsible minister should be required to certify that, at the time of disclosure, the information was properly classified. The prosecution would then be required to establish that the information was classified, but not that the disclosure of the information would harm the interests of the nation.[11]

5.14 As noted in Chapter 4, the 1988 White Paper issued by the UK Government Home Office did not agree with this approach.[12] Instead, the paper drew a distinction between disclosures of security and intelligence information by members of the security and intelligence services, and disclosures by others. The White Paper proposed that, in relation to disclosures by members of the security and intelligence services, there should be no requirement to prove damage. However, in relation to disclosures of information by individuals who were not members of the security and intelligence services, the prosecution should have to show that the disclosure was likely to cause damage.

5.15 Section 1 of the UK *Official Secrets Act* generally reflects the position set out in the 1988 White Paper. Section 1(4) defines a damaging disclosure of information relating to security or intelligence as follows:

> (a) it causes damage to the work of, or any part of, the security and intelligence services; or
>
> (b) it is of information or a document or other article which is such that its unauthorised disclosure would be likely to cause such damage or which falls within a class or description of information, documents or articles the unauthorised disclosure of which would be likely to have that effect.

---

10 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 56.

11 Ibid, 56.

12 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [75].

5.16 Section 2 of the *Official Secrets Act* defines a damaging disclosure of information relating to defence as follows:

> (a) it damages the capability of, or any part of, the armed forces of the Crown to carry out their tasks or leads to loss of life or injury to members of those forces or serious damage to the equipment or installations of those forces;
>
> (b) otherwise than as mentioned in paragraph (a) above, it endangers the interests of the UK abroad, seriously obstructs the promotion or protection by the UK of those interests or endangers the safety of British citizens abroad; or
>
> (c) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

5.17 In the Australian context, the *Review of the Commonwealth Criminal Law*, chaired by Sir Harry Gibbs (the Gibbs Committee) considered it appropriate to impose criminal sanctions in relation to the unauthorised disclosure of 'intelligence and national security information' without having to demonstrate harm. The Committee recommended that the prosecution should be required to prove harm in the case of a disclosure of information relating to defence.[13]

5.18 In the course of the Inquiry the ALRC also considered the need to define key concepts such as 'security' and 'defence'. Section 4(5) of the FOI Act contains a non-exhaustive definition of 'security of the Commonwealth' as follows:

> (a) matters relating to the detection, prevention or suppression of activities, whether within Australia or outside Australia, subversive of, or hostile to, the interests of the Commonwealth or of any country allied or associated with the Commonwealth; and
>
> (b) the security of any communications system or cryptographic system of the Commonwealth or of another country used for:
>
> (i) the defence of the Commonwealth or of any country allied or associated with the Commonwealth; or
>
> (ii) the conduct of the international relations of the Commonwealth.

5.19 The *FOI Guidelines—Exemption Sections in the FOI Act* (FOI Exemption Guidelines) provide further guidance on the meaning of national security in the FOI context:

> In broad terms, the 'security' of the Commonwealth refers to matters concerning the protection of Australia and its population from active measures of foreign intervention, espionage, sabotage, subversion and terrorism and the security of any communications system or cryptographic system of any country used for defence or conduct of international relations.[14]

---

13 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 323. This issue is discussed further in relation to specific secrecy offences in Ch 8.

14 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, 3.3.1.

5.20 The FOI Exemption Guidelines also note that the meaning of the term 'security' has arisen for consideration in a number of cases before the Administrative Appeals Tribunal (AAT) dealing with release of information under the FOI Act and the *Archives Act 1983* (Cth).[15]

5.21 Section 8 of the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) defines 'national security' to mean 'Australia's defence, security, international relations or law enforcement interests'. Section 9 goes on to state that for the purposes of the Act, the term 'security' has the same meaning as set out in s 4 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), namely:

> (a) the protection of, and of the people of, the Commonwealth and the several States and Territories from:
>
> (i) espionage;
>
> (ii) sabotage;
>
> (iii) politically motivated violence;
>
> (iv) promotion of communal violence;
>
> (v) attacks on Australia's defence system; or
>
> (vi) acts of foreign interference;
>
> whether directed from, or committed within, Australia or not; and
>
> (b) the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the subparagraphs of paragraph (a).

5.22 Section 4 of the ASIO Act further defines 'attacks on Australia's defence system' to mean:

> activities that are intended to, and are likely to, obstruct, hinder or interfere with the performance by the Defence Force of its functions or with the carrying out of other activities by or for the Commonwealth for the purposes of the defence or safety of the Commonwealth.

5.23 Neither the *National Security Information (Criminal and Civil Proceedings) Act* nor the FOI Act contain a separate definition of the term 'defence'.

5.24 The FOI Exemption Guidelines note, however, that decisions of the AAT have indicated that 'defence of the Commonwealth' includes meeting Australia's international obligations and ensuring the proper conduct of international defence relations; measures to deter and prevent foreign incursions into Australian territory; and the protection of the Defence Force from hindrance or activities which would prejudice its effectiveness. In addition, the AAT has indicated that to make a finding of 'damage' it needs to be presented with evidence that the release of information 'will

---

15 See, eg, *Re Slater and Cox* (*Director-General of Australian Archives*) (1988) 15 ALD 20; *Hocking and Department of Defence* (1987) 12 ALD 554; *Re Throssell and Australian Archives* (1987) 10 ALD 403.

enable possible enemies of good government to obtain knowledge of the security and defence measures used'.[16]

5.25 The general secrecy offence is intended to sit in the *Criminal Code.* Section 90.1 of the Code states that the security or defence of a country 'includes the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies'. However, this definition is situated in Part 5.2 of the Code and relates specifically to espionage and related offences.

5.26 As noted in Chapter 2, the right to freedom of expression may be restricted where necessary to protect national security according to art 19(3) of the *International Covenant on Civil and Political Rights* (ICCPR).[17] The *Siracusa Principles on the Limitation and Derogation Provisions in the ICCPR* (Siracusa Principles) state that the term 'national security' may be invoked to justify measures taken to protect the 'existence of the nation, its territorial integrity or political independence against force or threat of force'.[18]

Submissions and consultations

5.27 While stakeholders agreed that national security and defence should be included in the general secrecy offence, a number made submissions in relation to the requirement to prove that the disclosure caused, or was reasonably likely or intended to cause, damage. The AGD expressed the view that individual officers may not be in the best position to make a fully informed assessment of the risk of harm in the national security and intelligence context. The AGD stated that:

> In view of these factors, there is merit in considering specific secrecy offences that do not require harm to be established. These specific secrecy offences would protect those types of information where there is reasonable likelihood that harm will always be caused by unlawful disclosure. This could include national security and intelligence information as well as law enforcement information, consistent with the requirement under article 19(3) of the *International Covenant on Civil and Political Rights* that freedom of expression can be limited by law where necessary for the protection of national security or public order.[19]

5.28 Ron Fraser was firmly of the view, however, that:

> The Commission is correct on grounds of general penal principles not to except intelligence and national security information from the need for a harm test. A great deal of information may be properly described as such information, and its

16 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, 3.3.2.

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

18 United Nations Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4 (1984), [29].

19 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

> unauthorised disclosure will undoubtedly lead to various administrative and employment penalties for officers responsible, but criminal proceedings are not justified in the absence of specifiable harm or potential harm.[20]

ALRC's views

5.29 The ALRC's view is that the unauthorised disclosure of Commonwealth information that is reasonably likely, or intended, to damage the security or defence of the Commonwealth should be regulated by the criminal law.

5.30 In Chapter 8, the ALRC considers the specific secrecy offences prohibiting the disclosure of information obtained or generated by the intelligence agencies in connection with their functions, or relating to their functions. The ALRC concludes that these provisions—which do not require the prosecution to prove harm in every case—are justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies.[21]

5.31 The general secrecy offence, however, is intended to apply to all Commonwealth officers and to all Commonwealth information. As Fraser notes, a great deal of information has the potential to relate to national security or defence. In this broader context, it is the ALRC's view that the general secrecy offence should include an express harm requirement. The potential damage likely to be caused by disclosing such information may not be implicit in the information itself, or the context in which it is generated and used.

5.32 The ALRC recommends, therefore, that the general secrecy offence cover unauthorised disclosures that cause, are likely to cause or intended to cause, damage to the security or defence of the Commonwealth.

5.33 The ALRC has considered whether it is necessary to define the terms 'security' and 'defence' for the purposes of the general secrecy offence. In the ALRC's view, a definition of the term 'security' would assist Commonwealth officers and the courts to understand the scope of the offence. The definition set out in the ASIO Act is appropriate. This definition describes in concrete terms the activities and interests that the general secrecy provision is designed to protect. The term 'security' should, therefore, be defined for the purposes of the general secrecy offence by reference to the definition in the ASIO Act. This is consistent with the provisions of the *National Security Information (Criminal and Civil Proceedings) Act*.

5.34 The term 'defence of the Commonwealth' is more concrete and limited than 'security of the Commonwealth' and does not require a separate statutory definition. In addition, as noted above, the definition of 'security' in the ASIO Act includes 'attacks

---

20 R Fraser, *Submission SR 78,* 21 August 2009.

21 For example, *Australian Security Intelligence Organisation Act 1979* (Cth) s 18; *Intelligence Services Act 2001* (Cth) ss 39, 39A and 40.

on Australia's defence system', which is defined to mean activities that are intended to, and are likely to, obstruct, hinder or interfere with the performance by the Defence Force of its functions or with the carrying out of other activities by or for the Commonwealth for the purposes of the defence or safety of the Commonwealth.

5.35 In the ALRC's view, a secrecy offence framed and defined in this way will be consistent with Australia's obligations under art 19 of the ICCPR on the basis that it is necessary to protect the existence of the nation, its territorial integrity or political independence against force or threats of force. As always, however, the way the provision is enforced in practice will also need to be consistent with these obligations.

International relations

5.36 The Franks Committee recommended that criminal sanctions should apply to the unauthorised disclosure of official information relating to any matters which concern or affect foreign relations or the conduct of foreign relations.[22] As discussed above, the Franks Committee recommended the use of security classifications to indicate when the unauthorised disclosure of this information would be subject to criminal sanctions. The Gibbs Committee, on the other hand, recommended that the prosecution should be required to prove harm in the case of a disclosure of information relating to foreign relations.[23]

5.37 The 1988 White Paper recommended, and s 3 of the UK *Official Secrets Act* requires, that in order to attract criminal sanctions the disclosure of information relating to international relations must be damaging.[24] Section 3(2) provides that a disclosure is damaging if:

> (a) it endangers the interests of the UK abroad, seriously obstructs the promotion or protection by the UK of those interests or endangers the safety of British citizens abroad; or
>
> (b) it is of information or of a document or article which is such that its unauthorised disclosure would be likely to have any of those effects.

5.38 The FOI Exemption Guidelines provide guidance on what the concept means in the context of FOI:

> The phrase *damage to international relations* includes such things as intangible damage to Australia's reputation or relationships between government officials or loss of confidence or trust in the Government of Australia by an overseas government as well as loss or damage in monetary terms …

---

22 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 50.

23 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.50(c)].

24 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [50].

> The phrase international relations concerns the ability to maintain good working relations with other overseas governments and international organisations and to protect the flow of confidential information between them. …
>
> Lessening the confidence which another country would place on the government of Australia would satisfy the exemption (*Re Maher and Attorney-General's Department*), as would an expected reduction in the quality and quantity of information provided by a foreign government (*Re Wang and Department of Employment, Education and Training*).[25]

5.39 Section 10 of the *National Security Information (Criminal and Civil Proceedings) Act* defines 'international relations' to mean 'political, military and economic relations with foreign governments and international organisations'.

5.40 As noted in Chapter 2, according to art 19(3) of the ICCPR, the right to freedom of expression may be restricted where necessary to protect public order. The Siracusa Principles state that the term 'public order' is 'the sum of the rules which ensure the functioning of society or the set of fundamental principles on which society is founded' and that 'respect for human rights is part of public order'.[26] As noted above, it is also possible to restrict freedom of expression where necessary to protect 'national security'.

5.41 In DP 74, the ALRC included 'damage to international relations' in the proposed general secrecy offence, but expressed concern that imposing criminal liability on Commonwealth officers for disclosing information that harms, is reasonably likely to harm, or intended to harm Australia's international relations may be too broad. The ALRC noted that some such disclosures may cause only embarrassment, rather than significant harm.[27]

Submissions and consultations

5.42 Two stakeholders expressed support for including damage to international relations in the general secrecy offence.[28] However, Civil Liberties Australia (CLA) expressed the view that:

> It would be preferable to qualify the harm as clearly likely to have or intended to have substantial adverse effect on international relations. The FOI Draft Exposure Bill model, that expressly provides that embarrassment or loss of confidence must not be

---

25 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [3.3.3].

26 United Nations Commission on Human Rights, *The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, E/CN.4/1985/4 (1984), [29].

27 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), [7.64].

28 Attorney-General's Department, *Submission SR 67,* 14 August 2009; Australia's Right to Know, *Submission SR 35,* 6 March 2009.

taken into consideration in determining whether on balance, access would be contrary to the public interest, is an appropriate model to follow.[29]

ALRC's views

5.43 The ALRC's view is that the intentional unauthorised disclosure of information that is reasonably likely to damage the international relations of the Commonwealth should be regulated by the criminal law. The ALRC recommends that the term 'international relations' be defined by reference to the definition provided in s 10 of the *National Security Information (Criminal and Civil Proceedings) Act*, that is, 'political, military and economic relations with foreign governments and international organisations'. This means that the provision will be limited to unauthorised disclosures that damage, or are likely or intended to damage, Australia's political, military or economic relations with other countries or international organisations.

5.44 The ALRC acknowledges that this provision has the potential to be interpreted quite broadly. The ALRC has considered a range of mechanisms for restricting the scope of the provision including, for example, requiring that the disclosure have a 'substantial adverse effect' on international relations. The FOI Exemption Guidelines note that 'substantial adverse effect' has been interpreted to mean 'severe, of some gravity, large or weighty or of considerable amount, real or of substance and not insubstantial or nominal consequences'.[30] The ALRC is concerned that imposing a requirement that a disclosure have a 'substantial adverse effect' may exclude disclosures that cause damage such as a loss of confidence by foreign governments. Loss of confidence may not be viewed by the courts as sufficiently severe to constitute a substantial adverse effect on international relations. In the ALRC's view, however, such disclosures have the potential to cause real and significant damage to Australia's political, military or economic relations with other countries and therefore warrant the imposition of criminal sanctions.

5.45 A disclosure that embarrasses the Australian Government may also cause damage to Australia's international relations. For example, where a disclosure damaged Australia's reputation, as well as being 'embarrassing', it may lead to a loss of confidence or trust in Australia. A loss of confidence in the Australian Government's capacity to protect information is likely to result in a restricted flow of information from foreign governments. This, in turn, may impact on Australia's capacity to protect national security or on Australia's capacity to function in the global political, military and economic environment.

5.46 As noted above, prosecution under the general secrecy offence will only be consistent with Australia's international obligations under the ICCPR if it is necessary to protect national security, discussed above, or to ensure the functioning of Australian

---

29 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

30 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [1.1.6.1].

society (the protection of public order). In the ALRC's view, the protection of Australia's international relations is necessary to ensure that Australian society continues to function in the global environment, but a disclosure that *merely* embarrasses the Australian Government, without threatening real damage to international relations, is unlikely to meet the requirements of art 19 of the ICCPR.

Prejudicing the enforcement of the criminal law

5.47 In its report on s 2 of the UK *Official Secrets Act,* the Franks Committee noted that:

> The public have a right to information about such matters as general police methods and procedures, and prison treatment. These are matters of public interest, and Parliament and the people need adequate information to satisfy themselves that proper and effective measures are being taken and proper standards of behaviour are being observed. But the public have no right to information of a kind which would, for instance, be of direct use in the commission of an offence, or in evading detection or in escaping from prison. Such information requires effective protection.[31]

5.48 The Committee proposed that the criminal law should apply to the unauthorised disclosure of official information that is likely to be helpful in the commission of offences; is likely to be helpful in facilitating escape from legal custody; or likely to impede the prevention or detection of offences or the apprehension or prosecution of offenders.[32]

5.49 The 1988 White Paper agreed and noted that this description of the category of information to be protected 'already carries its own test of harm within it'. Section 4(2) of the *Official Secrets Act* applies to any information the disclosure of which:

> (a) results in the commission of an offence;
>
> (b) facilitates an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or
>
> (c) impedes the prevention or detection of offences or the apprehension or prosecution of suspected offenders.

5.50 Section 4 also applies to information obtained by the interception of communications under warrant, or by reason of any action authorised by warrant under the *Security Service Act 1989* (UK).

5.51 The Gibbs Committee expressed the view that 'because of the detailed statutory regime in Australia regulating the interception of telephone and telegraphic communications', it would be more appropriate to deal with the disclosure of this category of information in a specific provision relating to interception.[33] The

---

31 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 64.

32 Ibid, 65.

33 Section 63 of the *Telecommunications (Interception and Access) Act 1979* (Cth) is discussed in Ch 8.

Committee agreed, however, that the information protected by s 4(2) of the *Official Secrets Act* should also be protected in Australia.

5.52 Section 20A of the New Zealand *Summary Offences Act* establishes an offence for unauthorised communication of official information likely to:

- endanger the safety of any person;
- prejudice the maintenance of confidential sources of information in relation to the prevention, investigation, or detection of offences;
- prejudice the effectiveness of operational plans for the prevention, investigation, or detection of offences or the maintenance of public order, either generally or in a particular case; or
- prejudice the safe custody of offenders or of persons charged with offences.

5.53 Section 37(1)(a) of the FOI Act provides that certain information relating to the enforcement or administration of the law should be protected from disclosure. The section states 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.

5.54 Section 37(1)(b) provides that a document is an exempt document if disclosure would, or could reasonably be expected to, disclose 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.

5.55 In DP 74, the ALRC expressed the view that the disclosure of information that causes, is likely to cause, or is intended to cause harm to the prevention, detection, investigation, prosecution or punishment of criminal offences should be covered by the general secrecy offence. The formulation in s 37 of the FOI Act appeared, however, to be too wide for this purpose. The FOI Exemption Guidelines explain that s 37 extends to documents that relate to upholding or enforcing the civil law.[34] This highlights the policy differences between FOI legislation and criminal secrecy provisions. Under the FOI Act it is appropriate to protect from disclosure information that relates to all legal proceedings, including civil proceedings. In the ALRC's view, however, it is not

34 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [8.1.2].

appropriate to impose criminal sanctions for the disclosure of such information in the general secrecy offence.

5.56 The ALRC proposed instead to adopt a narrower formulation based in part on National Privacy Principle (NPP) 2 in the *Privacy Act 1988* (Cth). 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':[35]

- 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; or
- the protection of the public revenue.[36]

Submissions and consultations

5.57 In response to the Issues Paper, *Review of Secrecy Laws* (IP 34), 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.[37]

5.58 ACLEI stated 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

---

35 *Privacy Act 1988* (Cth) s 6 sets out a definition of 'enforcement body', which includes the Australian Federal Police (AFP), the Australian Crime Commission (ACC), the Australian Prudential Regulation Authority (APRA) and ASIC.

36 Ibid sch 3.

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

> compromised by unauthorised disclosure by individuals as a consequence of their corrupt conduct.[38]

5.59 In the view of the Australian Federal Police (AFP), the formulation proposed by the ALRC in DP 74 was too narrow:

> In our view the wording used by the ALRC to define this interest may be too narrow to cover all activities undertaken by law enforcement agencies. For example, the AFP's responsibilities under the *Family Law Act 1975* may not be adequately covered in the current formulation. In order to cover this type of interest a broader formulation along the lines of the FOI Act section 37(1)(a) may be necessary to include for example 'prejudice to the enforcement or proper administration of the law'.[39]

5.60 CLA, on the other hand, expressed the view that the proposed formulation was too wide and that the public interest protected should be limited to the enforcement of the criminal law. CLA suggested that the following elements should be removed: the enforcement of laws relating to the confiscation of the proceeds of crime, and the protection of the public revenue.[40]

5.61 The Australian Taxation Office (ATO) noted that the proposal to include the disclosure of information that prejudices the protection of the public revenue would be sufficient to protect internal ATO administrative documents, such as compliance risks and strategies, from disclosure.[41]

ALRC's views

5.62 The ALRC's view is that the recommended general secrecy offence should cover the disclosure of information that prejudices, or is likely or intended to prejudice, the prevention, detection, investigation, prosecution or punishment of criminal offences. A secrecy offence framed in this way will be consistent with Australia's obligations under art 19 of the ICCPR as it is necessary to protect the 'rules which ensure the functioning of society', including human rights and the rights of others. As always, however, the way the offence is enforced on a case-by-case basis will also have to be considered in light of Australia's international obligations under art 19.

5.63 In the ALRC's view, the formulation in s 37 of the FOI Act is too wide to provide a template for the general secrecy offence because it extends to the administration of any law, including the civil law. Where disclosures that impact on the enforcement of the civil law warrant the protection of the criminal law, this should be done in specific criminal offences that target particular information in specific contexts. The general criminal offence should not extend to unauthorised disclosures of information that would prejudice the enforcement of laws relating to the confiscation of the proceeds of crime, or the protection of the public revenue. Taxation legislation

---

38 Ibid.
39 Australian Federal Police, *Submission SR 70,* 14 August 2009.
40 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
41 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

and proceeds of crime legislation already contain specific secrecy offences targeting Commonwealth information in those contexts.[42]

5.64 In addition, the general criminal offence should not cover unauthorised disclosures of information that would prejudice the prevention, detection, investigation, prosecution or punishment of a breach of a law imposing penalties or sanctions that are not criminal. It would be excessive to impose criminal sanctions in the general secrecy offence for disclosures of information that threatened civil or administrative processes.

5.65 The ALRC recognises, however, that there may be some circumstances in which the disclosure of such information may warrant criminal sanctions—for example, in the area of corporate regulation where significant civil penalties are imposed for serious breaches of the law. In particular, this may be appropriate where civil penalties are included in provisions regulating entities as an alternative to criminal penalties because imprisonment is not an option in sentencing entities. In these circumstances, there may be a need for specific offences to protect the investigatory process. For example, the *Australian Securities and Investments Commission Act 2001* (Cth) makes it an offence to use or disclose records of witness examinations made in the course of an investigation, except in compliance with the conditions imposed by ASIC.[43] Any such specific secrecy offences should be considered in light of the ALRC's recommendations in Chapters 8 to 11.

5.66 The ALRC has not included elements in the general secrecy offence 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 penalties for such conduct. For example, under the law of contempt the courts may impose penalties for failure to comply with a court order, or an undertaking made to the court, restricting the publication of evidence adduced in closed proceedings.

Endangering the life or physical safety of any person

5.67 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.

5.68 As noted in Chapter 2, under art 19(3) of the ICCPR, the right to freedom of expression may be restricted where necessary to protect the rights of others.

---

42 *Proceeds of Crime Act 2002* (Cth) ss 210(1), (2); 217; 223(1), (2), (3); *Taxation Administration Act 1953* 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.

43 *Australian Securities and Investments Commission Act 2001* (Cth) ss 25, 26.

5.69 In DP 74, the ALRC proposed using a formulation based on s 37(1)(c) of the FOI Act, but suggested that 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'. There was some support expressed for including this element in the general secrecy offence.[44] Only one stakeholder expressed support for the broader language used in NPP 2.[45]

ALRC's views

5.70 The ALRC's view is 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. This kind of information might include, for example, the personal details of a police informant.[46] This approach recognises that disclosing information that endangers an individual's life or safety is a serious matter warranting criminal sanctions. A secrecy offence framed in this way will be consistent with Australia's obligations under art 19 of the ICCPR as it is necessary to protect the rights of others although, as always, it will be important to ensure that any prosecutions are brought in circumstances that are consistent with art 19.

5.71 The 'life, health or safety' formulation put forward in DP 74 was developed in the context of allowing, rather than restricting, disclosures of personal information under the *Privacy Act*. In the ALRC's view, unauthorised disclosures of information that are likely to endanger a person's health—for example, where the information was likely to exacerbate a mental health issue—should not generally attract criminal sanctions. Where the unauthorised disclosure would pose such a threat to a person's health that it would endanger their life or physical safety, the general secrecy offence would apply.

Prejudicing the protection of public safety

5.72 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.

5.73 As noted in Chapter 2, art 19(3) of the ICCPR states that freedom of expression may be restricted where necessary to protect public order, public health and the rights of others.

---

44 Attorney-General's Department, *Submission SR 36,* 6 March 2009; Australia's Right to Know, *Submission SR 35,* 6 March 2009.

45 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

46 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [8.5.6].

5.74 In DP 74, the ALRC proposed using a formulation based on NPP 2, that is, that the unauthorised disclosure would pose 'a serious threat to public health or public safety'. Only one stakeholder expressed support for the broader language used in NPP 2.[47]

ALRC's views

5.75 The ALRC's view is that a disclosure of Commonwealth information that prejudiced, was reasonably likely to prejudice, or intended to prejudice the protection of public safety should be covered by the general secrecy offence. This approach recognises that disclosing Commonwealth information that threatens public safety is a serious matter warranting a criminal penalty. A secrecy offence framed in this way will be consistent with Australia's obligations under art 19 of the ICCPR as it is necessary to protect public order and the rights of others although, as always, it will be important to ensure that any prosecutions are brought in circumstances that are consistent with art 19.

5.76 The ALRC has concluded that unauthorised disclosures of information that are likely to prejudice the protection of public health—for example, the location of national supplies of a vaccine being stockpiled in a secure location in case of national emergency—would also prejudice the protection of public safety. On this basis, the ALRC is not recommending the formulation put forward in DP 74 based on NPP 2.

Recommendation 5–1 The general secrecy offence should require that the disclosure of Commonwealth information did, or was reasonably likely to, or intended to:

(a) damage the security, defence or international relations of the Commonwealth;

(b) prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;

(c) endanger the life or physical safety of any person; or

(d) prejudice the protection of public safety.

47 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

Recommendation 5–2 The terms 'security' and 'international relations' should be defined for the purposes of the general secrecy offence by reference to the relevant provisions of the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth).

What should not be included in the general secrecy offence?

5.77 In the following section, the ALRC considers which of the public interests protected by the various FOI Act exemptions should *not* be protected by the general secrecy offence.

Cabinet documents and internal working documents

5.78 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 a decision of the Cabinet has been officially published.[48]

5.79 Section 35 provides an exemption for Executive Council documents, although the ALRC notes that the FOI Exposure Draft Bill proposes the repeal of this section.[49] Section 36 provides an exemption for internal working documents, that is, documents that 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.[50]

---

48 The Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) 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) Act 2009* (Cth) sch 1 cl 8 repealed the provisions of the FOI Act that permitted the Secretary of the Department of the Prime Minister and Cabinet to issue a conclusive certificate in relation to documents exempt under s 34.

49 *Freedom of Information Act 1982* (Cth) s 35; Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2 cl 23.

50 *Freedom of Information Act 1982* (Cth) s 36. Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2 cll 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) Act 2009* (Cth) sch 1 cl 10 repealed the provisions of the FOI Act that permitted a minister or delegate to issue a conclusive certificate in relation to documents exempt under s 36(1).

5.80 In the UK, the Franks Committee noted the argument that ministers, their advisers and public servants must be able to exchange views fully and frankly among themselves without the risk that the details of such exchanges will be made public. The Committee accepted that there were grounds for protecting this kind of information. It did not accept, however, that criminal sanctions should be used to give general protection to the internal processes of government, stating that 'the discipline of the public service is in our view an adequate means, as well as being the appropriate means, of dealing with such matters'.[51]

5.81 The Committee noted, however, that the arguments about free and frank discussion were said to apply with special force to Cabinet documents:

> The ultimate responsibility for the decisions of the Government lies in the Cabinet. The Cabinet works on the doctrine of collective responsibility. Whatever the individual views of its members, when the Cabinet reaches a decision it is the decision of them all. Each shares in the collective responsibility for that decision. Anything which damages this collective unity and integrity of the Cabinet damages the government of the country. Privacy for the internal deliberations of the Cabinet, it is argued, is an essential condition of the collective unity. Cabinet Ministers must be able to discuss matters with their colleagues in an uninhibited way. It is in the nature of the system that Cabinet Ministers are sometimes overruled by the colleagues, and sometimes change their minds. Equally, a variety of possible policies and courses of action may have to be considered before one is decided upon. It was put to us that such a system is not strengthened by exposure to the public eye. On the contrary, when confidentiality among colleagues in the Cabinet is lost, discussion will be less free and less frank. Its quality will be impaired and so may the quality of decisions reached.[52]

5.82 The Committee recommended that the criminal law should apply to Cabinet documents, but not to official papers on the same subject or draft Cabinet documents, on the basis that criminal sanctions are imposed to protect the collective responsibility of Cabinet, rather than the content of the documents.[53]

5.83 The 1988 White Paper, however, expressly rejected the argument that criminal sanctions should apply to the unauthorised disclosure of Cabinet documents:

> The Government remains of the view, which was also taken in 1979, that it is not necessary or right for criminal sanctions to apply to Cabinet documents as a class or to advice to Ministers as a class. Documents of this kind will be protected by the proposals if their subject matter merits it, but their coverage *en bloc* would fuel suspicions that information was being protected by the criminal law merely for fear of political embarrassment.[54]

---

51 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 67.

52 Ibid, 68.

53 Ibid, 69.

54 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [32].

5.84 The UK *Official Secrets Act* does not impose criminal sanctions for the unauthorised disclosure of Cabinet documents or internal working documents of government. The Gibbs Committee agreed that 'information in [Cabinet] documents should only be protected by criminal sanctions if they fall within other descriptions of protected documents'.[55]

5.85 The *Freedom of Information Act 2000* (UK) takes a different approach from the Australian FOI Act in relation to disclosure of internal government documents, indicating that such documents do not require absolute protection. The UK Act includes exemptions for documents relating to the formulation of government policy[56] and ministerial communications,[57] but provides that, in order for these exemptions to be maintained in any particular case, the public interest in maintaining the exemption must outweigh the public interest in the disclosure of the information.[58]

5.86 In a 2008 decision, confirmed on appeal, the UK Information Commissioner allowed the release of a number of Cabinet documents—with some redactions—recording meetings of Cabinet which considered legal advice provided by the Attorney-General in relation to military action against Iraq.[59] The Commissioner stated that the factors in favour of disclosure were:

- the gravity and controversial nature of the subject matter;
- accountability for government decisions;
- transparency of decision making; and
- public participation in government decisions.

5.87 The Commissioner expressed the view that:

> In respect of effects on Cabinet collective responsibility, disclosure of the minutes will not set a dangerous precedent in respect of other Cabinet minutes. This is because the Commissioner accepts that the protection of the convention of Cabinet collective responsibility is, in general terms, a strong factor favouring the withholding of Cabinet minutes.
>
> In this case the Commissioner considers the public interest in transparency, accountability, public debate and understanding of decisions made to be more important considerations than that in the importance of being able to discuss policy issues without inhibition.[60]

---

55 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.18].

56 *Freedom of Information Act 2000* (UK) s 35(1)(a).

57 Ibid s 35(1)(b).

58 Ibid s 2(2)(b).

59 Information Commissioner, *Decision Notice FS50165372—Cabinet Office (19 February 2008)* (2008) <www.ico.gov.uk> at 3 September 2009.

60 Ibid, 10.

5.88 The ALRC did not include Cabinet documents, Executive Council documents, or internal working documents in the general secrecy offence proposed in DP 74. This was on the basis that the offence should generally target harms, rather than categories of information, and that the internal processes of government, including the Cabinet process, did not warrant the protection of the criminal law. Although it is important to protect such documents, the ALRC's view was that the protection should be provided by administrative processes and disciplinary penalties, rather than criminal sanctions.

Submissions and consultations

5.89 The AGD acknowledged the ALRC's preferred position that the general secrecy offence should not expressly protect categories of information, but stated that:

> the unauthorised 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.[61]

5.90 The AGD expressed the view that, because Cabinet documents do not fit easily into agency-specific legislation, it would be preferable to include this category of information in the general secrecy offence.

5.91 On the other hand, the ARTK coalition was of the view that:

> In any event, it is clear that decision making processes of government should not be nested in secrecy. The experience in jurisdictions where those processes are open to public scrutiny has been that it results in more professional, apolitical and reasoned decision making. That is to be encouraged[62]

ALRC's views

5.92 In light of the Australian Government's commitment to open government, the ALRC's view is that Cabinet documents, Executive Council documents and internal working documents should be protected by administrative processes—such as classification and information-handling guidelines—and the imposition of administrative penalties, rather than criminal sanctions. Unauthorised disclosure of these categories of Commonwealth information may be 'prejudicial to the effective working of government', but it is essentially a disciplinary, rather than a criminal, matter.

5.93 As discussed in Chapter 4, the ALRC's view is that, in the context of the general secrecy offence, categories of information should not be protected. However, if disclosure of a Cabinet, Executive Council or internal working document caused, was likely to cause, or was intended to cause harm to one of the specified public interests listed in the general offence it would be caught by the offence.

---

61 Attorney-General's Department, *Submission SR 67,* 14 August 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009.

62 Australia's Right to Know, *Submission SR 72,* 17 August 2009.

Information communicated in confidence

Information communicated in confidence by a foreign government

5.94 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, an authority of the Commonwealth or a person receiving the communication on behalf of the Commonwealth or of an authority of the Commonwealth.[63]

5.95 In the UK, the 1988 White Paper proposed that secrecy offences should apply to information obtained in confidence from other governments and international organisations as a category of information, without the need to prove that the disclosure caused harm.[64] While the *Official Secrets Act* was based to a large extent on the approach outlined in the White Paper, the Act takes a different approach on this issue. Section 3(1)(b) of the Act provides that it is an offence to make a damaging disclosure of 'any confidential information, document or other article which was obtained from a State other than the UK or an international organisation'.

5.96 Section 3(3) goes on to provide that, in the case of information covered by s 3(1)(b), the fact that the information is confidential, or the nature of its contents, may be sufficient to establish that the disclosure would be damaging.

5.97 In Australia, the Gibbs Committee recommended that the prosecution should be required to prove that the disclosure of information obtained in confidence from foreign governments and international organisations caused harm.[65]

5.98 In DP 74, the ALRC argued that, for the purposes of the general secrecy offence, it was not appropriate to protect categories of information as such. The particular problems with protecting this category of information are highlighted by the FOI Exemption Guidelines, which state that:

> There is no requirement to show that the foreign government continues to maintain confidentiality in respect of the document; the issue is simply whether the document was communicated in confidence at the time (*Re Robinson and Department of*

---

63 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) 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.

64 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [51].

65 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 331. 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: H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 332.

> *Foreign Affairs*). The document will be exempt even if the matter is no longer confidential at the time when access is sought (*Secretary, Department of Foreign Affairs v Whittaker*).
>
> Because information need only be *communicated in confidence*, even the existence of the information in the public domain will, in some cases, not affect the exempt status of the document (*Commonwealth of Australia v Hittich*; *Re Rees and Australian Federal Police*).[66]

Submissions and consultations

5.99 The AGD noted the Gibbs Committee recommendation that information received in confidence from foreign governments should be a protected category of information:

> As well as having a deterrent effect, the inclusion of information provided in confidence by a foreign government in a general secrecy offence will provide assurance to foreign governments that their information will be appropriately protected. We are not convinced that the harm to international relations element of the general secrecy offence would be sufficient to cover all such information, and would not provide sufficient assurance to foreign governments. This could negatively impact on current and future arrangements for the sharing of information and intelligence by foreign governments with Australia.[67]

5.100 The Australian Transaction Reports and Analysis Centre (AUSTRAC) expressed in-principle support for a general secrecy offence that incorporated a harm element with respect to specified public interests, but expressed reservations about the distinction the ALRC drew between international relations and information communicated in confidence by a foreign government or international organisation:

> AUSTRAC believes that any disclosure of information provided by a foreign government or international organisation on the express understanding that its confidentiality will be protected has the potential to disrupt the future exchange of information, and therefore should automatically be categorised as protected information.[68]

5.101 AUSTRAC stated that it received confidential information from international organisations, such as the Financial Action Task Force, the Asia/Pacific Group on Money Laundering and the Egmont Group of financial intelligence units. AUSTRAC noted that, while international organisations have a regulatory role in terms of global standard setting and ensuring compliance in this area, the information received from international organisations is not covered by the secrecy provisions in the *Anti-Money Laundering and Counter Terrorism Act 2006* (Cth). The provisions only cover information communicated by governments, or government agencies and authorities.[69]

---

66 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [3.5.3]–[3.5.4].

67 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

68 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

69 Ibid.

ALRC's views

5.102 The ALRC recognises 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 exchange of information between governments and international organisations is an essential element of international relations. If Commonwealth information was disclosed in circumstances that had the potential to, or did in fact, damage that flow, one would have a strong argument that the disclosure had caused, or was reasonably likely to cause, damage to international relations. In this way, the disclosure would be caught by the general secrecy offence.

5.103 The ALRC remains of the view that, for the purposes of the general secrecy offence, it is not appropriate to protect categories of information without expressly stating the harm the prohibition on disclosure is seeking to prevent. Not every document communicated in confidence by a foreign government or international organisation would damage international relations if disclosed. For example, the information communicated in confidence may have become less sensitive with the passage of time or in the course of events.

5.104 Section 3 of the UK *Official Secrets Act* requires that the disclosure of such information must be damaging to international relations, but goes on to state that the fact that the information is confidential—or the nature or contents of the information—may be sufficient to establish that the disclosure is damaging. This approach does not protect information communicated in confidence as a category. Rather it ensures that criminal charges may be brought only where the information remains confidential, or is otherwise damaging, at the time the information is disclosed.

5.105 The fact that information is confidential at the time of disclosure is not conclusive of damage, but *may* be sufficient to establish damage. It is not necessary to state this expressly in the general secrecy offence, but the point could be made in the Explanatory Memorandum and Second Reading Speech accompanying the general secrecy offence.

Information communicated in confidence by a state or territory

5.106 Section 33A of the FOI Act provides that a document is an exempt document if disclosure:

> (a) would, or could reasonably be expected to, cause damage to relations between the Commonwealth and a state; or

> (b) 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.[70]

5.107 The public interests protected by this provision are not of the same order as those protected by, for example, s 33 of the FOI Act—national security, defence and international relations. Section 33A(5) of the Act expressly acknowledges that there will be situations in which the disclosure of documents protected by this exemption will be in the public interest. This is not the case, for example, in relation to documents protected by s 33. The Gibbs Committee was of the view that:

> The relations between an Australian State and the Commonwealth Government are on a totally different plane from the relations between Australia and a foreign country … The Review Committee is not persuaded that it is necessary to include a further category of protected information based on section 33A of the *Freedom of Information Act 1982*.[71]

5.108 On this basis, the ALRC did not include 'damage to relations between the Commonwealth and the states and territories' or 'information communicated in confidence by or on behalf of the states or territories' in the general secrecy offence proposed in DP 74. The issue was not raised in submissions.

5.109 For the reasons discussed above, the general secrecy offence should not include protected categories of information, such as information communicated in confidence. While the ALRC acknowledges that information damaging to relations between the Commonwealth and the states and territories requires protection, unauthorised disclosure of this kind of information should be addressed through intergovernmental arrangements, the imposition of administrative sanctions, or the pursuit of general law remedies. Where such information is sensitive for other reasons—for example, because it relates to national security, the enforcement of the criminal law, or public safety—unauthorised disclosures may be caught by other elements of the general secrecy offence.

Material obtained in confidence

5.110 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

---

70 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) 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) Act 2009* (Cth) sch 1 cll 6–7 repealed the provisions of the FOI Act that permitted a minister or delegate to issue a conclusive certificate in relation to documents exempt under s 33A(1).

71 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.15]–[31.16].

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.

Personal and commercial information

5.111 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)'.[72]

5.112 Section 43 of the FOI Act provides that a document is an exempt document if its disclosure would disclose:

> (a) trade secrets;
>
> (b) 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
>
> (c) information (other than trade secrets or information to which paragraph (b) applies) concerning a person in respect of his or her business or professional affairs or concerning the business, commercial or financial affairs of an organization or undertaking, being information:
>
> (i) 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 organization or undertaking in respect of its lawful business, commercial or financial affairs; or
>
> (ii) the disclosure of which under this Act 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.[73]

5.113 In 1972, the Franks Committee recommended that criminal sanctions should be available in relation to unauthorised disclosure of personal and commercial information. The Committee noted that governments require increasing amounts of information from individuals and organisations. The information is provided on the basis that it will be kept confidential, and individuals and organisations have a right to expect that it will be protected. Governments cannot function effectively without the information and any breakdown of trust between government and people would have

---

72 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2 cll 24, 28 propose 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.

73 Ibid sch 3 pt 2 cll 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.

adverse repercussions on the government of the country. In addition, the Committee noted that 'there is no tension in this sphere between openness and secrecy. Everything points to the need for full and effective protection'.[74]

5.114 The Committee stated that individuals and organisations that suffer damage from an unauthorised disclosure of their private information should also be able to pursue civil remedies, but deterrence of public servants and the reassurance provided to citizens is more appropriately provided by the criminal law.[75]

5.115 The 1988 White Paper, however, took a different approach. The paper noted that sensitive personal and commercial information provided to government should be given adequate protection:

> But the Government has concluded that it would not be right to give blanket protection to all information offered in confidence in legislation designed to protect only that information the disclosure of which would seriously harm the public interest.[76]

5.116 The paper expressed the view that, generally, civil remedies and disciplinary procedures were a more appropriate response to disclosures of private personal or commercial information. The paper noted, however, that there are specific circumstances—particularly where information is provided under a statutory requirement—where it is in the public interest to give personal and commercial information the protection of the criminal law. The paper stated that there were a number of existing offences relating to disclosure of specific information provided under statutory requirements, and noted that consideration would be given to the need to create other specific offences.[77]

5.117 The Gibbs Committee agreed, noting that the basic purpose of the proposed secrecy offence was to impose criminal sanctions for unauthorised disclosure of information that would seriously harm the public interest. The Gibbs Committee was of the view that, where personal and commercial information required protection, it should be protected by specific provisions such as those under social security and taxation legislation.[78]

Discussion Paper 74 proposals

5.118 In DP 74, the ALRC agreed, in principle, with the position put by the Gibbs Committee that, generally, personal and commercial information should not be

---

74 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 73.

75 Ibid, 74.

76 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [34].

77 Ibid, [35].

78 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.13].

protected 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 Information Privacy Principles (IPPs) or NPPs, and administrative, contractual and general law obligations apply in relation to both personal and commercial information.

5.119 However, there was significant concern expressed by government agencies about the ability of the Australian Government to collect personal and commercial information from the Australian community. Agencies 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.

5.120 In response to these concerns, the ALRC proposed to include personal privacy and the protection of business, commercial or financial affairs as two of the interests to be protected by the general secrecy offence.[79] In order to warrant criminal penalties, however, the ALRC proposed that the harm to personal privacy or commercial interests should be of a relatively high order, that is, the disclosure would have to have a 'substantial adverse effect' on personal privacy or on a person's lawful business, or professional affairs or on the business, commercial or financial affairs of an organisation.

Submissions and consultations

5.121 A range of views were expressed in the course of the Inquiry relating to whether or not to include personal and commercial information in the ambit of the general secrecy offence.

In support of including personal and commercial information

5.122 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.[80]

5.123 The AGD stated 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 regulate the behaviour of individuals. The AGD noted that some overlap exists, but that the processes and remedies available under the *Privacy Act*,

---

79 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 7–1.

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

which are aimed at agencies and organisations, do not have the same deterrent effect for individual Commonwealth officers.[81]

5.124 A number of agencies that handle large amounts of personal information, including the Department of Human Services (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 deterrent value of criminal penalties.[82]

5.125 The Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) noted the highly sensitive nature of the personal information it collects under social security, family assistance and child support legislation stating that:

> FaHCSIA considers that any unauthorised disclosure, regardless of whether there is any intention of harm against a specified public interest in a particular instance, would inherently harm the public interest. This is because any unauthorised disclosure would have the potential to erode public confidence in the protection of information held in Departmental records … It is possible that lack of public confidence in the protection of customer's sensitive personal information could lead to attempts to withhold relevant information.[83]

5.126 A number of other stakeholders agreed 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.[84]

5.127 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.[85]

5.128 Similarly, the Australian Competition and Consumer Commission (ACCC) stated that, in contrast to many Australian Government agencies, the ACCC is mainly concerned with commercially sensitive information, the disclosure of which 'may have a substantial adverse effect on the information provider'.[86]

---

81 Ibid.

82 Department of Human Services, *Submission SR 26,* 20 February 2009; Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.

83 Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.

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

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

86 Australian Competition & Consumer Commission, *Submission SR 11,* 12 February 2009.

5.129 The Office of the Privacy Commissioner noted that the *Privacy Act* provides for the investigation and conciliation of complaints made by individuals regarding a breach of the IPPs by an agency.[87] In making a determination in response to a complaint, the Privacy Commissioner may declare that the agency 'should perform any reasonable act or course of conduct to redress any loss or damaged suffered by the complainant'[88] or that the 'complainant is entitled to a specified amount by way of compensation for any loss or damaged suffered'.[89] By way of contrast, the Office noted that secrecy provisions regulate the conduct of individuals, rather than agencies, and do not seek to 'remedy the personal loss or address the specific damage suffered by an individual in the event that their personal information is wrongfully disclosed'.[90]

5.130 The Office expressed the view that robust protection of personal information held by government was essential to ensure community confidence and continued engagement with government. The Office acknowledged the ALRC's view that unauthorised disclosure of personal information generally should not attract criminal penalties and suggested that 'in many instances, administrative penalties could act as a sufficient deterrent against inappropriate handling and disclosure of personal information', but noted that criminal penalties may also be appropriate in some circumstances. The Office did offer in-principle support for including personal privacy in the general secrecy offence, in light of the concerns expressed by agencies about the need to protect such information.[91]

Concern about 'substantial adverse effect'

5.131 The AGD expressed some concern over the ALRC's proposal to limit the offence to disclosures that have a 'substantial adverse effect' on personal privacy, querying how this might be interpreted by the courts and what factors might be taken into account in determining the effect of a disclosure. The AGD suggested a two-tier approach in which the first tier would address unauthorised disclosures of personal information that cause harm to an individual and the second tier would address such disclosures that had a substantial adverse effect on personal privacy.[92]

87 *Privacy Act 1988* (Cth) s 27(1)(a).
88 Ibid s 52(1)(b)(ii).
89 Ibid s 52(1)(b)(iii).
90 Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009.
91 Ibid.
92 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

5.132 The AFP had similar concerns, expressing the view that the requirement would be hard to define and difficult to prove:

> Restricting the secrecy offence protections for private interests in this way will hamper criminal prosecutions and diminish the confidence of the private sector in the Government's ability to protect and handle personal and commercial information. In our view there are strong reasons against creating a 'substantial adverse effect' limitation on the protection of private interests. If such a limitation is created then the term 'substantial adverse effect' should be defined in non-exhaustive terms within the proposed offence provisions to provide guidance to the judiciary and prosecuting authorities on the meaning of the term.[93]

5.133 Indigenous Business Australia (IBA) expressed similar concerns about the proposed threshold:

> As drafted, the general offence will rarely, if ever, apply to unauthorised disclosures of information held by IBA, creating an environment that contains no effective mechanism for holding individuals liable for serious unauthorised disclosures.[94]

5.134 IBA noted that the *Privacy Act* does not bind individuals and that, because the Act covers only 'personal information', its effect is limited in relation to commercial information. IBA further stated that general law or equitable remedies, such as breach of confidence, were highly technical. IBA did not accept that the general secrecy offence should establish a higher threshold of harm for privacy and commercial interests, noting that this was not consistent with the approach in the FOI Act and may give rise to evidential difficulties for the prosecution.[95]

5.135 The Commonwealth Director of Public Prosecutions (CDPP) agreed, stating that:

> From a prosecution perspective, we are uncertain what will be required to be proved to make out an offence based on a disclosure which has a substantial adverse effect on personal privacy. It may be that this limb of the offence requires some additional assistance to make clear what the offence encompasses, such as a definition of 'personal privacy' and/or 'substantial adverse effect'.[96]

5.136 The DHS expressed concern that the proposed formulation would make it 'difficult to be confident that a prosecution would succeed in any but the most extreme situations' and that this would reduce the practical significance of the provisions. In addition, the DHS noted that the proposed formulation in relation to personal and commercial information:

> gives no recognition to the important public interests which may be *indirectly* adversely affected by disclosures. In particular, a disclosure may damage community confidence in Government's commitment and ability to safeguard such sensitive

---

93 Australian Federal Police, *Submission SR 70,* 14 August 2009.
94 Indigenous Business Australia, *Submission SR 64,* 13 August 2009.
95 Ibid.
96 Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009.

> information and community cooperation in providing such information to Government.[97]

5.137 The DHS suggested that the general secrecy offence be extended to include disclosures that have a substantial adverse effect on the delivery of government services, adding that:

> A related concern is the need to deal with situations where there is a course of conduct and/or a group of disclosures. For example, a malicious or disaffected employee of an agency may engage in a pattern of disclosure of protected personal or business/professional information over a period of time or in a concentrated burst of activity. It may be that none of the disclosures taken in isolation would reach the 'substantial adverse effect' threshold but that the cumulative effect of the disclosures could be substantial.[98]

5.138 The Australian Privacy Foundation suggested that 'substantial' set too high a threshold and should be replaced with 'significant' or 'material'.[99] The Department of Health and Ageing expressed concern that the test proposed would cause uncertainty, be inappropriate in some circumstances, and provide insufficient protection for certain types of personal health information.[100]

Concerns about including personal and commercial information

5.139 Ron Fraser stated that, generally, there should not be criminal penalties for unauthorised disclosure of information causing harm to individual or corporate interests, and noted that the Gibbs Committee did not recommend addressing these harms through the criminal law. He suggested that disclosure of confidential personal and commercial information should continue to be regulated by the *Privacy Act*, and by non-criminal statutory obligations of secrecy such as those set out in reg 2.1 of the *Public Service Regulations*. He noted that use of the 'substantial adverse effect' threshold would help to ensure that criminal penalties were not applied where the disclosure of information had only minor or trivial consequences.[101]

5.140 The ARTK coalition submitted 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

97 Department of Human Services, *Submission SR 83,* 8 September 2009.
98 Ibid.
99 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.
100 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.
101 R Fraser, *Submission SR 78,* 21 August 2009.

> adequate to deter a breach of the duty of confidence. The same should apply in the public sector.[102]

5.141 The ARTK coalition stated that it was unnecessary to criminalise disclosures which have a substantial adverse effect on personal privacy or commercial affairs and that doing so would lead to 'a significant chilling of free speech in Australia'.[103] The coalition noted that, in the private sector, the disclosure of confidential information attracted civil remedies such as damages, or administrative penalties such as dismissal. The ARTK coalition was of the view that the same approach should be adopted in the public sector, noting that the individual loss or harm caused by such disclosures is not addressed by the imposition of criminal sanctions.

5.142 Civil Liberties Australia expressed the view that unauthorised disclosure of personal information or disclosures that harm business, commercial or financial affairs should not generally attract criminal penalties, and that the existing range of remedies under general, contract and administrative law are sufficient. CLA stated that:

> It is inconsistent for criminal sanctions, including imprisonment, to apply to a person operating in the public sphere when they would not apply to a person not operating in the public sphere for the same act.[104]

5.143 CLA was not convinced by the argument that criminal penalties were necessary to ensure public confidence in government systems that collect personal information.[105]

ALRC's views

5.144 The ALRC has decided not to recommend that the general secrecy offence cover disclosures that have a substantial adverse effect on personal privacy or commercial affairs.

5.145 Where personal or commercial information is disclosed in the private sector, the matter may give rise to contractual, common law or equitable remedies. In the ALRC's view, where personal or commercial information is disclosed in the public sector, the same sort of avenues of redress should generally be available—including the lodging of a complaint under the *Privacy Act*, the imposition of administrative penalties, and contractual, common law and equitable remedies.

5.146 Where the disclosure involves fraud—that is, the information is disclosed with the intention of dishonestly obtaining a benefit or dishonestly causing a detriment to another person—s 142.2 of the *Criminal Code* provides criminal sanctions.

---

102 Australia's Right to Know, *Submission SR 72,* 17 August 2009; Australia's Right to Know, *Submission SR 35,* 6 March 2009.

103 Australia's Right to Know, *Submission SR 72,* 17 August 2009.

104 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

105 Ibid.

5.147 A number of agencies, such as the ATO, DHS, APRA and the ACCC, collect large amounts of personal and commercial information. Although some of this information can be collected under statutory compulsory powers, in many cases agencies rely on the voluntary provision of information. These agencies expressed the view that it is necessary to protect this information with secrecy offences in order to ensure this essential flow of information to the government.

5.148 The ALRC agrees that, in some cases, it is appropriate to protect this information with criminal secrecy provisions. It is not, however, appropriate to do this in the general secrecy offence. In the ALRC's view, the public interest being protected—that is, the relationship of trust between government and the people—is not an interest that could easily be articulated in, and protected by, the general secrecy offence. It would be very difficult to prove beyond reasonable doubt, for example, that a single disclosure of personal or commercial information had any impact on this public interest.

5.149 For this reason, the ALRC's view is that in specific regulatory contexts—for example, taxation, social security or corporate regulation—where it can be demonstrated that a relationship of trust is crucial to the operations of government, it may be appropriate for specific secrecy offences to protect specific categories of information. The circumstances in which such specific secrecy offences will be justified are discussed in detail in Chapters 8 to 11.

Financial or property interests of the Commonwealth

5.150 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.[106] As noted above, the ALRC's view is that, generally, disclosures of Commonwealth information should not attract criminal sanctions where they would not attract such sanctions outside the public sector. This information, which is in the nature of confidential commercial information, should therefore be protected by appropriate administrative processes and penalties and the general law.

Information affecting the economy

5.151 Section 44(1) 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

106 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2 cll 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.

- 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.

5.152 Section 44(2) states that the kinds of documents to which s 44(1) may apply include, but are not limited to, documents containing matter relating to:

(a) currency or exchange rates;

(b) interest rates;

(c) taxes, including duties of customs or of excise;

(d) the regulation or supervision of banking, insurance and other financial institutions;

(e) proposals for expenditure;

(f) foreign investment in Australia; or

(g) borrowings by the Commonwealth, a State or an authority of the Commonwealth or of a State.

5.153 The FOI Exemption Guidelines note 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.[107]

5.154 The FOI Exposure Draft Bill proposes to repeal s 44 of the FOI Act and enact new s 47J in its place. The proposed s 47J differs from s 44 in that it 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, an agency or minister must give a person access to these documents unless it would be contrary to the public interest.[108]

5.155 The Franks Committee expressed the view that the possibility of harm to the economy should not generally attract sanctions under the criminal law:

> There are aspects of economic management which the Government properly keeps secret, though in many instances the information in question is eventually made public. But the fact that an unauthorised disclosure would damage the economy rather

---

107 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [16.1.3].

108 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2 cll 24, 28.

> than some other aspect of the national life, does not distinguish economic management from the rest of the Government's ordinary domestic functions. Here, as with these other domestic functions, reliance can properly be placed on all the other means of protection available, without involving the ultimate sanctions of the criminal law.[109]

5.156 The Committee noted, for example, that while governments take precautions to protect Budget information—including limiting access to the information—the harm caused by premature unauthorised disclosure of such information is likely to be political embarrassment, rather than harm to the economy of the nation. For this reason, the Committee was of the view that such disclosures should not attract criminal sanctions.[110] Where such information is disclosed in order to gain a benefit or cause a detriment, the Committee expressed the view that this should be covered by a different offence:

> Our proposal is not that governments should no longer protect economic and financial information of this kind. It is that those leaking such information should no longer be liable to prosecution and imprisonment, unless it is done for private gain.[111]

5.157 The Committee did, however, express the view that official information relating to 'any proposals, negotiations or decisions connected with alterations in the value of sterling, or relating to the reserves, including their extent or any movement in or threat to them' should be protected by the criminal law. This was on the basis that crises involving the exchange rate or the reserves had the potential to cause 'exceptionally grave injury to the economy' and the life of the nation and thus justified the imposition of criminal sanctions.[112]

5.158 The 1988 White Paper stated, however, that it was not necessary to protect economic information as a class, noting that protection would be provided by disciplinary processes and penalties and, where necessary, by specific legislation on particular subjects.[113] The UK *Official Secrets Act* does not include provisions imposing criminal sanctions for this kind of information.

5.159 The Gibbs Committee agreed that the disclosure of information that would cause substantial damage to the national economy should not be covered by a secrecy offence. This was on the basis that public access to information about the economy was crucial, and that the chilling effect of a criminal offence in this context was not justified on the balance of public interests. The Committee was convinced by

---

109 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 51.

110 Ibid, 52.

111 Ibid, 53. The use of Commonwealth information with the intention of dishonestly obtaining a benefit or causing a detriment is already a criminal offence under s 142.2 of the *Criminal Code* (Cth).

112 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 51.

113 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [33].

arguments put in submissions, including one from the Treasury, which stated that the risk of an unauthorised disclosure damaging the national economy was very small, and that the breadth of the formulation would give rise to 'unforeseen uses of the offence by future governments and their servants'.[114] The Treasury was of the view that administrative sanctions were an appropriate response to the unauthorised disclosure of this kind of information.

5.160 Section 20A of the New Zealand *Summary Offences Act*, however, does establish an offence for unauthorised communication of official information likely to seriously damage the economy of New Zealand by prematurely disclosing decisions to continue or change economic or financial policies relating to:

(i) exchange rates or the control of overseas exchange transactions;

(ii) the regulation of banking or credit;

(iii) taxation;

(iv) the stability, control, and adjustment of prices of goods and services, rents, and other costs, and rates of wages, salaries, and other incomes;

(v) the borrowing of money by the Government of New Zealand; or

(vi) the entering into of overseas trade agreements.

5.161 However, the maximum penalty for this offence is only three months imprisonment, or a fine of $2,000.

ALRC's views

5.162 The ALRC is not recommending that 'substantial adverse effect on the ability of the Government of the Commonwealth to manage the economy of Australia'—the current FOI Act formulation—or 'substantial adverse effect on Australia's economy'—the new formulation proposed in the FOI Exposure Draft Bill—be included in the general secrecy provision.

5.163 Information that has the potential to have an adverse effect on Australia's economy is protected by administrative processes and penalties, as well as the general law. The issue is whether unauthorised disclosure of this kind of information warrants the imposition of criminal sanctions in the general secrecy offence. The Franks Committee was of the view that a small subset of information, relating to the value of the currency and the reserves, did warrant the protection of the criminal law, but the UK Government did not agree, and this information is not included in the UK *Official Secrets Act*. The Gibbs Committee indicated that, on balance, it was not appropriate to impose criminal sanctions for the unauthorised disclosure of this kind of information. The ALRC agrees. The potential scope of the provision would be too uncertain, and may have an unacceptable chilling effect on the flow of information in an area in which there is a strong public interest in openness and accountability.

---

114 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [30.10].

5.164 The New Zealand legislation does impose criminal penalties for unauthorised disclosure of particular information, but stipulates a low maximum penalty of three months imprisonment or a $2,000 fine. The ALRC notes that the AGD *Guide to Framing Commonwealth Offences* states that maximum penalties of less than six months should be avoided, to underline the fact that imprisonment is reserved for serious offences.[115]

5.165 The ALRC also notes that under s 47J of the FOI Exposure Draft Bill, documents that would, or could reasonably be expected to, have a substantial adverse effect on Australia's economy are 'conditionally exempt' documents. Other documents that are classified as conditionally exempt in the Bill are those relating to Commonwealth-state relations; the deliberative process; the financial or property interests of the Commonwealth; certain operations of agencies; personal privacy; business affairs; and research. Where a document is classified as 'conditionally exempt', access must be provided unless providing access would, on balance, be contrary to the public interest. This indicates that, in the Australian Government's view, the public interest balance in relation to disclosing this information is different from the public interest balance in disclosing documents affecting, for example, national security, defence, international relations, or law enforcement.

5.166 While the ALRC's view is that this kind of information should not be protected in the general secrecy offence, it may be appropriate to protect more specific information in a specific secrecy offence. Chapters 8 to 11 of this report consider the circumstances in which specific secrecy offences are justified.

Other FOI exemptions

Documents to which secrecy provisions apply

5.167 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 16.

Documents concerning certain operations of agencies

5.168 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;

---

115 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 42.

- 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.[116]

5.169 These are matters relating to the internal management and operations of agencies, and the protection of information relating to these matters 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.[117]

Sections 42, 46, 47 and 47A of the FOI Act

5.170 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; would amount to a contempt of court, or infringe the privileges of parliament; arise out of certain elements of the companies and securities legislation;[118] 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 powers and procedures to deal with unauthorised disclosure of documents, including the ability to impose penalties.

5.171 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. Finally, the electoral roll and related documents are regulated by specific secrecy provisions. The circumstances in which specific secrecy offences may be justified are discussed in Chapters 8 to 11.

---

116 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) 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.

117 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.

118 Ibid 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.

6. General Secrecy Offence: Elements

Contents

Introduction

6.1 In Chapter 4 the ALRC recommends that ss 70 and 79(3) of the *Crimes Act 1914* (Cth) be repealed, and that a number of new, more targeted, offences should be enacted in the *Criminal Code* (Cth).[1] In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC proposed a range of offences addressing the disclosure of Commonwealth information by Commonwealth officers, and the subsequent disclosure

1 Sections 70 and 79(3) are described in detail in Chs 3 and 4, and set out in full in Appendix 5.

of such information by any other person who disclosed the information knowing that it had been originally disclosed in breach of the law.[2]

6.2 In this chapter, the ALRC considers some of the elements of those offences, including whose conduct, and what kind of conduct, should be regulated. The ALRC also recommends a new offence for the subsequent disclosure of Commonwealth information by any person who receives the information in confidence. Chapter 7 goes on to consider what exceptions and defences should be available under the recommended offence provisions, and what penalties should apply for breach.

Whose conduct should be regulated?

6.3 Chapter 3 provides an overview of the parties regulated by existing federal secrecy provisions. As noted in that chapter, secrecy provisions can apply to:

- Commonwealth employees;
- organisations or individuals providing services for or on behalf of the Commonwealth;
- Commonwealth agencies;
- other specific categories of organisations or individuals; or
- 'any person'.

6.4 In this section, the ALRC considers whether the 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 new offence.

'Commonwealth officer' under the *Crimes Act*

6.5 Section 70 of the *Crimes Act* applies to a 'Commonwealth officer', defined in s 3 of that 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;

2 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposals 8–1 and 8–3.

> (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.[3]

6.6 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 Force (ADF) and the Australian Postal Corporation.

'Commonwealth public official' under the *Criminal Code*

6.7 The *Criminal Code* includes a number of offences concerning the conduct of a 'Commonwealth public official'.[4] The term 'Commonwealth public official' is defined exhaustively in the Dictionary to the Code, and includes elements from all three branches of government—the executive, the legislature and the judiciary.[5] 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.[6]

---

3 *Crimes Act 1914* (Cth) s 3.

4 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.

5 The definition is set out in full in Appendix 5.

6 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [367].

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'.[7]

6.8 The definition includes bodies established 'by or under a law of the Commonwealth' created to perform government functions. 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'.[8]

6.9 A number of bodies and organisations are expressly excluded because they are separate from the Commonwealth government. These include Indigenous councils and associations; the ACT, Northern Territory and Norfolk Island Governments; and corporations and bodies such as registered unions and employer associations.[9]

ALRC's views

6.10 The executive branch of government collects and generates vast amounts of information. In particular, the executive collects information from and about private individuals on both a voluntary and compulsory basis. It is this sector that is the main focus of s 70 of the *Crimes Act*. In the ALRC's view, the new general secrecy offence should also regulate the disclosure of information by officers of the executive branch.

6.11 Although both the legislative and judicial branches collect information from individuals and organisations, 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 to protect 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.[10]

6.12 The definition of 'Commonwealth public official' in the *Criminal Code* includes officials from all three branches of government, but 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 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

---

7 Ibid.
8 Ibid.
9 See, eg, *Criminal Code* (Cth) dictionary, definition of 'Commonwealth public official' paras (n) and (r).
10 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 90(4) re disclosure to the courts and *Migration Act 1958* (Cth) s 46A(5) re disclosure to the Australian Parliament.

office, while the general secrecy offence is directed at protecting information held 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 general secrecy offence. Instead, 'Commonwealth officer' should be defined separately for the purposes of the proposed new offence.

6.13 The following section examines the categories of people covered by 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 categories should be incorporated into the definition of 'Commonwealth officer' for the purposes of the new general secrecy offence.

Public sector employees

6.14 The following categories are taken from the definition of 'Commonwealth public official' in the *Criminal Code*. They cover APS employees and other public sector employees and, although the categories are not defined in exactly the same way as their equivalents in the *Crimes Act*, there is a significant degree of overlap:

- APS employees;
- other individuals employed by the Commonwealth otherwise than under the *Public Service Act 1999* (Cth);
- 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.

6.15 These categories represent the key working units of the executive branch of government that are responsible for collecting, generating and controlling the flow of Commonwealth information. The extent to which these categories cover judicial officers is discussed further below.

6.16 In DP 74, the ALRC proposed that these categories form the core of the definition of 'Commonwealth officer' for the purposes of the general secrecy offence.

A number of stakeholders expressed support for this proposal.[11] The ALRC recommends that the definition of 'Commonwealth officer' include these elements of the definition of 'Commonwealth public official'.

Contracted service providers

6.17 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.[12] It recognises that Commonwealth information is often handled by those contracted to provide goods and services to or on behalf of the Commonwealth.

6.18 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 of 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.[13]

6.19 The definition of 'Commonwealth public official' in the Dictionary to 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.

---

11 Community and Public Sector Union, *Submission SR 57,* 7 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

12 *Statute Law (Miscellaneous Provisions) Act 1987* (Cth) sch 1. This issue is discussed further in Ch 2.

13 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [371]–[372].

6.20 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.

6.21 These provisions are specifically directed to individuals, rather than entities. There is an argument, in the context of the general secrecy offence, that entities that are contracted service providers should also be subject to the offence. The Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) (the Tax Laws Exposure Draft Bill) defines 'taxation officer' broadly to include:

> an entity engaged to provide services relating to the [Australian Taxation Office (ATO)] (such as cleaning firms or IT contractors) and any individual employed or subcontracted by such an entity.[14]

Submissions and consultations

6.22 There was considerable support in submissions for ensuring that the proposed general secrecy offence continues to cover Commonwealth contracted service providers.[15] 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* [*1988* (Cth)], 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.[16]

6.23 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.[17]

---

14 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [2.8]. See Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-25. The contractual relationship between the Australian Government and contracted service provider entities and individuals is discussed in Ch 13.

15 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.

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

17 The Treasury, *Submission SR 22,* 19 February 2009.

6.24 The Australian Intelligence Community (AIC)[18] suggested that this element could be expanded to cover persons who have 'any contract, agreement or arrangement' with the Commonwealth, to reflect the width of the relevant provisions of the *Intelligence Services Act 2001* (Cth)[19] and the *Australian Security Intelligence Organisation Act 1979* (Cth)[20] in this regard.[21] The Department of Health and Ageing (DoHA) was also concerned that the provision was not wide enough and would not cover, for example, external members of departmental committees and researchers who receive information for the purposes of research.[22]

ALRC's views

6.25 The ALRC agrees that Commonwealth contracted service providers should be covered by the new general secrecy offence. This reflects the reality that contracted service 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 were collected or generated by an Australian Government agency, and has the potential to cause the same kind and degree of harm if disclosed without authority. 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.

6.26 The ALRC recommends, therefore, that the definition of 'Commonwealth officer' for the purposes of the general secrecy offence should include individuals and entities that 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.

6.27 In Chapter 13, the ALRC recommends that contracted service providers should take steps to ensure that contractors' employees who have access to Commonwealth information are made aware of their obligations of secrecy, including the circumstances in which criminal liability could result.

6.28 The ALRC does not recommend, however, that the definition be broadened to include any person who has an 'agreement or arrangement' with the Commonwealth. Such provisions feature in the specific secrecy offences governing the AIC. Given the

---

18 The Australian Intelligence Community is made up of six agencies: the Australia Secret Intelligence Service; the Australian Security Intelligence Organisation (ASIO); the Defence Intelligence Organisation (DIO); the Defence Imagery and Geospatial Organisation; the Defence Signals Directorate; and the Office of National Assessments (ONA).

19 *Intelligence Services Act 2001* (Cth) ss 39(1)(b)(ii), 39A(1)(b)(ii) and 40(1)(b)(ii).

20 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2).

21 Australian Intelligence Community, *Submission SR 77,* 20 August 2009.

22 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.

context and the nature of these agencies, individuals entering into an agreement or arrangement to share information—no matter how informal the arrangements might be—should have been made aware of the sensitive nature of the information involved and the implications of unauthorised disclosure.

6.29 In the wider public sector context, an 'agreement' or 'arrangement' of itself is not sufficient, in the ALRC's view, to impose potential criminal liability under the general secrecy offence on persons who are not otherwise 'Commonwealth officers'. In this context, something more is warranted to ensure that the parties understand that the information is being disclosed in confidence, and the reasonable likelihood that a subsequent unauthorised disclosure will be harmful. The ALRC recommends, below, an offence for the unauthorised subsequent disclosure of information that has been disclosed by a Commonwealth officer to a non-Commonwealth officer on terms requiring it to be held in confidence, where the subsequent disclosure causes, or is reasonably likely to cause, harm to one of the essential public interests set out in Recommendation 5–1.[23] This offence is intended to cover parties who are not 'Commonwealth officers' but who are given access to Commonwealth information on a confidential basis—such as external departmental committee members or researchers.

The Governor-General

6.30 The Governor-General belongs to the executive branch of government and has access to Commonwealth information at the highest level. 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.[24]

6.31 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 certain circumstances, as the provision applies to any person.

6.32 In DP 74, the ALRC proposed that, although the Governor-General is not currently subject to s 70 of the *Crimes Act*, the conduct of the Governor-General should be regulated by the new general secrecy offence.[25] The ALRC did not receive any submissions in relation to this issue, and recommends that the Governor-General

---

23 Recommendation 6–7.

24 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [371].

25 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 8–1.

should be included in the definition of 'Commonwealth officer' for the purposes of the general secrecy offence.

6.33 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 officer' developed for the purposes of the new offence. 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*'.

Ministers and parliamentary secretaries

6.34 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.[26] 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'.[27]

6.35 As with the Governor-General, ministers and parliamentary secretaries belong to the executive branch of government and have access to Commonwealth information at the highest level.[28] Some specific secrecy offence provisions, such as s 150 of the *Child Support (Assessment) Act 1989* (Cth), expressly apply to ministers. Ministers and parliamentary secretaries are also potentially subject to prosecution under s 79(3) of the *Crimes Act*. It is arguable, therefore, that the activity of ministers and parliamentary secretaries should be regulated by the new general secrecy offence.

6.36 The 1972 United Kingdom (UK) departmental committee chaired by Lord Franks (the Franks Committee) was of the view that, while ministers largely authorise themselves to disclose official information, they are under the same duty as public servants to protect information that may be damaging, and should be covered by secrecy provisions.[29]

---

26 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [371].

27 *Wong v Minister for Immigration and Multicultural and Indigenous Affairs* (2004) 204 ALR 722, 744.

28 Parliamentary secretaries are ministers: *Ministers of State Act 1952* (Cth) s 4.

29 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 78.

6.37 On the other hand, ministers are sometimes required to decide whether or not it is in the public interest to disclose certain information. A minister may decide to release information 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.[30]

Submissions and consultations

6.38 The ALRC received only a few submissions on this issue but Harry Evans, the Clerk of the Senate, noted that the proposed general secrecy offence would not apply to ministers and parliamentary secretaries in respect of their participation in parliamentary proceedings.[31] This is because such disclosures are protected by parliamentary privilege.[32]

6.39 In his submission, Dr 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.[33]

6.40 The Australian Privacy Foundation agreed.[34]

ALRC's views

6.41 The ALRC recommends that, for the purposes of the 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 recommends in Chapter 7 that one of the exceptions to the new general secrecy offence should be disclosure with the approval of the responsible minister, who would have to certify that disclosure is in the public interest in any particular case.[35]

6.42 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*' and, as such, will fall within the definition of 'Commonwealth officer' for the purposes of the new general

---

30 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 62.
31 Clerk of the Senate, *Submission SR 48,* 31 July 2009.
32 Parliamentary privilege and its interaction with secrecy provisions is discussed in detail in Ch 16.
33 J Renwick, *Submission SR 02,* 11 December 2008.
34 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.
35 Recommendation 7–1(b).

secrecy offence. Although the exception for approval by the minister will allow some information to be disclosed by ministerial staff, this will not protect ministers' staff from prosecution for unauthorised 'leaks' where information is disclosed without the minister's authority.

Former Commonwealth officers

6.43 Section 70 of the *Crimes Act* expressly regulates the behaviour of persons who are Commonwealth officers,[36] as well as those who have been Commonwealth officers.[37]

6.44 As noted in Chapters 3 and 13, the common law duty of loyalty and fidelity provides some protection for information acquired during the employment relationship once that relationship ends. Leo Tsaknis notes 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.[38]

6.45 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 expresses the view that this imposes 'a form of servitude that the common law would not countenance' on former officers.[39] Paul Finn agreed with this view, stating that this provision is 'objectionably wide in its scope and mysterious in its possible applications'.[40]

Submissions and consultations

6.46 In DP 74, the ALRC proposed that the general secrecy offence should apply to both current and former Commonwealth officers.[41] A number of stakeholders expressed support for this position,[42] some noting that it would significantly undermine the utility of the provisions if they did not extend to former officers.[43] The Australian Prudential Regulation Authority (APRA), for example, stated that the effectiveness of

---

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.

41 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 8–1.

42 Australian Federal Police, *Submission SR 70,* 14 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

43 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.

its secrecy provision would be 'dramatically curtailed if it did not apply to former officers'.[44]

6.47 In response to the Issues Paper, *Review of Secrecy Laws* (IP 34), the Australian Government Attorney-General's Department (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.[45]

6.48 The Australian Securities and Investments Commission 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.[46]

ALRC's views

6.49 The ALRC's view is that the 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, for example, in the AIC or law enforcement contexts. The requirement, discussed in Chapter 5, that to attract criminal liability any disclosure must cause harm, be reasonably likely to cause harm, or be intended to cause harm will limit the circumstances in which former Commonwealth officers will be liable.

Members of the Houses of Parliament

6.50 Members of the Australian Parliament—both senators and members of the House of Representatives—who are not ministers or parliamentary secretaries, form part of the legislative, rather than the executive, branch of government. 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 certain circumstances.

---

44 Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.
45 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
46 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.

6.51 The general secrecy offence targets Commonwealth information held by Commonwealth officers. In DP 74, the ALRC did not propose extending the definition of Commonwealth officer beyond the executive branch to include Members of Parliament who are not ministers or parliamentary secretaries. The ALRC did not receive any specific feedback on this point and is not recommending that the definition of Commonwealth officer should include Members of Parliament. Members of Parliament may, however, be liable to criminal penalties if in breach of the subsequent disclosure offences discussed below.[47]

6.52 In addition, Members of Parliament are liable to criminal penalties for breach of other provisions of the *Criminal Code.* These include provisions that prohibit a Commonwealth public official from using any information that was obtained in his or her 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.[48]

Commonwealth judicial officers

6.53 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.[49]

6.54 Judicial officers, when acting judicially, do not form part of the executive branch of government, but comprise the judicial branch. 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 branches of government: the legislature, the 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 government. General secrecy provisions must not, therefore, interfere with, or limit, the exercise of federal judicial power by a federal court.

6.55 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). In *Grollo v Palmer*, Gummow J expressly considered this situation and the fact

---

47 Recommendations 6–6, 6–7.

48 *Criminal Code* (Cth) s 142.2.

49 Revised Explanatory Memorandum, Criminal Code Amendment (Theft, Fraud, Bribery and Related Offences) Bill 2000 (Cth), [370].

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.* In this case, Gummow J found 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' but noted that his decision rested on the construction of the particular provisions under consideration.[50]

6.56 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.[51]

ALRC's views

6.57 The general secrecy offence targets Commonwealth information held by Commonwealth officers in the executive branch of government. The ALRC does not recommend that the definition of Commonwealth officer be extended beyond the executive branch to include judicial officers acting in their judicial capacity. However, judicial officers may be liable under the general secrecy offence when appointed as designated persons to perform executive functions under Commonwealth legislation, to the extent that this is consistent with the exercise of federal judicial power.

6.58 In addition, the ALRC recommends the enactment of two offences prohibiting the subsequent disclosure of Commonwealth information by any person, where the person receives the information in confidence, or knowing that, or reckless as to whether, the information has been disclosed in breach of the general secrecy offence.[52] These offences 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 requirement not to interfere with the exercise of judicial power, and the doctrine of parliamentary privilege.

Recommendation 6–1 The 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);

50 *Grollo v Palmer* (1995) 184 CLR 348, 398.
51 *Criminal Code* (Cth) s 142.2.
52 Recommendations 6–6, 6–7.

(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; or

(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.

What conduct should be regulated?

6.59 The following section considers what conduct should be covered by the general secrecy offence. At present, approximately half of Commonwealth secrecy provisions regulate activities other than (but usually in addition to) the disclosure of information—including soliciting,[53] receiving,[54] obtaining,[55] possessing,[56] making a record of,[57] or using[58] 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.[59]

6.60 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

53 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 165.
54 See, eg, *Crimes Act 1914* (Cth) s 79(6).
55 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 163.
56 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9.
57 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.
58 See, eg, *Aged Care Act 1997* (Cth) s 62-1.
59 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32.

offence;[60] aiding, abetting, counselling or procuring the commission of an offence by another person;[61] incitement, where a person urges the commission of an offence;[62] and conspiracy, where a person conspires with another person to commit an offence.[63]

6.61 If a new criminal offence for disclosure of Commonwealth information by Commonwealth officers were included in the *Criminal Code*, as recommended in this Report, 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.

6.62 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.[64] In DP 74, the ALRC proposed that the general secrecy offence should be limited to the disclosure of Commonwealth information, while noting that, in some specific contexts it may be appropriate to regulate a wider range of activity. The ALRC argued that a great deal of conduct that may precede an unauthorised disclosure, such as recording or copying information, should be dealt with through administrative procedures and penalties. In addition, some 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.

6.63 In the following section, the ALRC considers activity other than disclosure of Commonwealth information—including receiving, copying, recording and using information—and whether this conduct should be covered by the general secrecy offence. The issues and submissions received are considered under three headings: receiving information; copying, recording and using information; and disclosing, divulging and communicating information. The ALRC's views in relation to conduct are set out at the end of the discussion. This section is also relevant to the subsequent disclosure offences—which cover the unauthorised disclosure of Commonwealth information by non-Commonwealth officers in some circumstances. These offences are considered further below.[65]

Receiving information

6.64 The ALRC's mapping exercise identified seven secrecy provisions that criminalise the possession or receipt of information.[66] The House of Representatives Standing Committee on Legal and Constitutional Affairs has cautioned against the creation of offences for the mere possession or receipt of confidential information. In

60 *Criminal Code* (Cth) s 11.1.
61 Ibid s 11.2.
62 Ibid s 11.4.
63 Ibid s 11.5.
64 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–4.
65 Recommendations 6–6, 6–7.
66 See eg *Crimes Act 1914* (Cth) s 79(4)–(6); *Defence (Special Undertakings) Act 1952* (Cth) s 9(2).

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'.[67]

Submissions and consultations

6.65 A number of stakeholders expressed concern about offences that extended to unsolicited possession or receipt of information.[68] 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.[69]

6.66 The Public Interest Advocacy Centre agreed that it would be undesirable to criminalise the 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.[70]

6.67 The AFP, on the other hand, expressed the view that unauthorised receipt and retention of information should be covered, particularly where the person in receipt of the information is aware that the disclosure to them was unlawful.[71]

Copying, recording and using information

6.68 A number of secrecy provisions regulate conduct potentially leading up to an unauthorised disclosure of information, such as copying and recording 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 organisation; while a 'disclosure' refers to the release of information to those outside an organisation.[72]

---

67 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].

68 Law Council of Australia, *Submission SR 30,* 27 February 2009; The Treasury, *Submission SR 22,* 19 February 2009.

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

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

71 Australian Federal Police, *Submission SR 70,* 14 August 2009.

72 Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), NPP 2.

6.69 The Tax Laws Exposure Draft Bill covers both the recording and disclosure of taxpayer information.[73] 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'.[74]

Submissions and consultations

6.70 A number of stakeholders suggested 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 1953* (Cth) 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.[75]

6.71 The Department of Education, Employment and Workplace Relations noted that, although 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.[76]

6.72 The AIC noted that the 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. The espionage offences in s 91.1 of the *Criminal Code* also apply to unauthorised making, obtaining or copying a record. The AIC considered it essential to preserve these elements in the intelligence context.[77]

---

73 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-20.

74 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.15].

75 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

76 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.

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

Disclosing, divulging and communicating information

6.73 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

6.74 The ATO and APRA submitted that disclosure should be the primary mischief addressed by secrecy provisions.[78] 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.[79]

6.75 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.[80]

6.76 The DHS also drew attention to 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* [*1953* (Cth)]*, Health Insurance Act* [*1973* (Cth)]), 'disclosing or producing' (*Medical Indemnity Act* [*2002* (Cth)]), and 'disclosing' only (*Aged Care Act* [*1997* (Cth)]*, Dental Benefits Act* [*2008* (Cth)]). 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.[81]

6.77 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'.[82]

---

78 Australian Taxation Office, *Submission SR 13,* 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.

79 R Fraser, *Submission SR 42,* 23 March 2009.

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

81 Ibid.

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

6.78 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.[83]

ALRC's views

6.79 The ALRC agrees with the AGD that the focus of the new offences 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 5 would arise only from unauthorised disclosure of Commonwealth information. 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.

6.80 While the ALRC recommends that the new general secrecy offence should be limited to 'disclosure' of Commonwealth information, Chapter 9 considers the circumstances that might justify applying criminal sanctions to other conduct in specific secrecy offences. The ALRC recognises that in some contexts, such as national security, offences that cover conduct other than disclosure may be necessary to prevent harm to an essential public interest. These are context-specific provisions, however, and this approach is not appropriate in general provisions applying to all Commonwealth information.

6.81 How information is 'used' within an agency is a different and wider issue than simply protecting the information from unauthorised disclosure. A clear distinction between use and disclosure is drawn in the Privacy Commissioner's guidelines, discussed above. 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.

6.82 The ALRC's view is that the mere receipt or possession of information should not be covered in the general secrecy offence or the subsequent disclosure offences. However, where information is received in confidence or in breach of the general secrecy offence, and subsequently disclosed in circumstances that are unauthorised and likely to harm essential public interests, the ALRC has recommended a number of 'subsequent disclosure' offences, discussed below.[84]

---

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

84 Recommendations 6–6, 6–7.

6.83 The ALRC's view is that a great deal of conduct that may precede an unauthorised disclosure, such as recording or copying information, should 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 a diary, where the conduct is discovered before any disclosure has occurred, would appear to be of this order.[85] 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.

Recommendation 6–2 The general secrecy offence should regulate the disclosure of Commonwealth information as defined in Recommendation 6–3.

What information should be protected?

6.84 In Chapter 3, the ALRC considers the various categories of information protected by the hundreds of existing secrecy provisions in federal legislation.[86] In this section, the ALRC considers what information should be protected by the new general secrecy offence and the subsequent disclosure offences.

6.85 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.

6.86 Regulation 2.1 of the *Public Service Regulations 1999* (Cth), the administrative secrecy provision that applies to APS employees, covers 'information which the APS employee obtains or generates in connection with the APS employee's employment'.

6.87 The *Australian Government Protective Security Manual*[87] binds all Commonwealth agencies to a series of procedures designed to protect 'official information' which includes any information received or collected by, or on behalf of, the Government, through its agencies and contractors.[88]

6.88 Other possible models include s 142.2 of the *Criminal Code*, which prohibits a 'Commonwealth public official' from dishonestly using information 'obtained in the

85 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.15]. This issue is discussed further in Ch 9.
86 See also Ch 9.
87 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual (PSM)* (2005).
88 Ibid, pt C, [1.3].

official's capacity as a Commonwealth public official'. Section 18(2) of the *Australian Security Intelligence Organisation Act 1979* (Cth) (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'.

6.89 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).[89]

6.90 In DP 74 the ALRC proposed that the 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.[90]

Submissions and consultations

6.91 A number of stakeholders expressed support for the ALRC's proposal, on the ground that it was important to ensure that the provision provides protection for a wide range of information, including information that has not been accessed legitimately.[91]

ALRC's views

6.92 The ALRC recommends retaining a broad definition of Commonwealth information in the 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 complement more specific provisions that are limited in their scope to particular parties or particular information.

6.93 The formulation used in the *Criminal Code*—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

---

89 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [2.17].

90 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 8–6.

91 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

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.

6.94 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 to which the officer may have 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.

6.95 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 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 recommends 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'.

Recommendation 6–3 The 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 Recommendation 6–1.

Fault elements

6.96 The *Criminal Code* sets out the structural framework for Commonwealth criminal offences. The Code provides that offences have physical elements, for example, conduct, and fault elements, such as intention, knowledge, recklessness or negligence.[92] Under the Code, if the legislation creating an offence does not specify a fault element for a physical element consisting of conduct, the automatic fault element is intention.[93] Where an offence provision does not specify a fault element for a physical element consisting of a circumstance or a result, the automatic fault element is recklessness.[94] In the following section the ALRC considers what fault elements should attach to the core physical elements of the general secrecy offence.

92 *Criminal Code* (Cth) s 5.1.
93 Ibid s 5.6(1).
94 Ibid s 5.6(2).

Fault element attaching to disclosure

6.97 The ALRC's mapping exercise indicates that the majority of Commonwealth secrecy provisions, including s 70 of the *Crimes Act*, do not stipulate fault elements. Therefore, on the basis of the provisions of the *Criminal Code*, the fault element attaching to the conduct of publishing or communicating information under s 70 of the *Crimes Act* is intention. In DP 74, the ALRC proposed that the fault element attaching to disclosure in the general secrecy offence should also be intention, that is, the prosecution would have to establish that the act of disclosure was intentional.[95]

6.98 The ALRC considered whether the offence should also include recklessness as a fault element in relation to the unauthorised disclosure of Commonwealth information. Section 5.4 of the *Criminal Code* provides that:

> (1) A person is reckless with respect to a circumstance if:
>
> (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.

6.99 If the offence was framed to cover reckless disclosure, the prosecution would be required to prove that the accused was aware of a substantial risk that disclosure would occur as the result of the accused's conduct and, having regard to the circumstances known to him or her, it was unjustifiable to take the risk.

6.100 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

95 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 8–5.

(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.[96]

6.101 The AGD *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that:

> criminal law policy provides that the fault elements supplied by the *Criminal Code* should apply unless there is a justifiable reason for departing from them. Departure from the principles set down in the Code would normally only be considered appropriate where it was not possible to achieve Parliament's intention through the *Criminal Code* options.[97]

6.102 The Guide also notes that 'it will almost always be clear and incontestable that a person intended his or her own conduct'.[98] In DP 74, the ALRC asked for stakeholder views on whether it would be appropriate to include recklessness as to disclosure as part of the general secrecy offence.[99]

Submissions and consultations

6.103 A small number of stakeholders made submissions on this issue. DoHA expressed support for the proposal that the fault element attaching to disclosure should be intention.[100] The AFP, on the other hand, was of the view that the general secrecy offence should cover reckless, as well as intentional, disclosure of Commonwealth information, noting that s 79(4)(c) of the *Crimes Act* currently extends to reckless conduct:

> For example, if a disgruntled Commonwealth employee deliberately left a USB drive containing confidential Commonwealth information in a train station hoping that someone would find it and publicly disclose its contents, it may be hard to argue that the employee intentionally disclosed the information.[101]

ALRC's views

6.104 The ALRC recommends that the fault element attaching to the act of disclosure in the general secrecy offence should be intention. This is the existing situation under s 70 of the *Crimes Act* and the vast majority of other secrecy offences. It is also consistent with the policy position in the *Guide to Framing Commonwealth Offences*, discussed above. The ALRC can see no justification for a departure from the automatic fault element stipulated in the *Criminal Code*.

---

96 See also *Crimes Act 1914* (Cth) s 3ZQJ.

97 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 22.

98 Ibid.

99 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), [8.113].

100 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.

101 Australian Federal Police, *Submission SR 70,* 14 August 2009.

Recommendation 6–4 The general secrecy offence should require intention as the fault element attaching to the physical element consisting of disclosure.

Fault element attaching to harm

6.105 Both the general secrecy offence and the subsequent disclosure offences, discussed below, require that the prosecution prove that the unauthorised disclosures caused harm, or were reasonably likely to cause harm, to one of the specified public interests. Where conduct causes harm, that harm may be characterised as a 'result' within the framework established by the *Criminal Code*. The Code provides that where an offence provision does not specify a fault element for a physical element consisting of a result, the fault element is recklessness.[102] The Code also provides that if recklessness is the fault element for a physical element of an offence, proof of intention, knowledge or recklessness will satisfy that fault element.[103]

6.106 On the basis of the automatic fault elements set out in the *Criminal Code*, the general secrecy offence would consist of an intentional disclosure of Commonwealth information by a Commonwealth officer who knew, intended or was reckless as to whether the disclosure would cause, or was reasonably likely to cause, harm to the identified public interests.

6.107 In DP 74, the ALRC proposed that the general secrecy offence should include three tiers.[104] The first tier was to cover an intentional disclosure of Commonwealth information by a Commonwealth officer, with strict liability attaching to the harm element. The prosecution would not be required to prove that the Commonwealth officer knew, intended or was reckless as to whether the disclosure would cause harm, simply that the disclosure did, or was reasonably likely to, cause harm. The ALRC also proposed a more serious offence that would require the prosecution to prove that the officer knew, intended or was reckless as to whether the disclosure would cause harm, or was reasonably likely to cause harm.

Strict liability and absolute liability

6.108 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

---

102 *Criminal Code* (Cth) s 5.6(2).

103 Ibid s 5.4(4).

104 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 7–2. In this report the ALRC is not recommending a tiered general secrecy offence. The second tier offence proposed in DP 74 covered disclosures that were damaging to personal privacy or commercial interests. As discussed in Ch 5, the ALRC is not recommending that such disclosures be covered by the general secrecy offence.

relation to absolute liability offences.[105] Courts are unlikely to impose strict or absolute liability unless there is a clear and express indication in the legislation.[106]

6.109 The *Guide to Framing Commonwealth Offences* notes that the automatic fault elements set out in 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).[107]

6.110 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.[108]

6.111 The Senate Standing Committee for the Scrutiny of Bills 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 consideration and on a case-by-case basis.[109] The Standing Committee concluded that strict liability may be appropriate where it has proved difficult to prosecute fault provisions, particularly those involving intent. The Standing 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 is peculiarly within the knowledge of the defendant.[110]

6.112 The 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.[111]

6.113 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 1982* (Cth). This 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 knew, intended, or was reckless as to whether, the disclosure

---

105 *Criminal Code* (Cth) ss 6.1, 6.2. See also *Proudman v Dayman* (1941) 67 CLR 536.

106 *He Kaw Teh v The Queen* (1985) 157 CLR 523.

107 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 24.

108 Ibid, 25.

109 Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002), 283.

110 Australian Parliament—Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002), 259.

111 Ibid, 285.

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.

6.114 The first-tier general secrecy offence proposed in DP 74 would have required the prosecution to prove that:

- a Commonwealth officer intentionally disclosed Commonwealth information; and
- the disclosure harmed, or was reasonably likely to harm, the essential public interests set out in Recommendation 5–1.

6.115 However, the prosecution would not have to prove that the officer knew, intended or was reckless as to whether the disclosure would cause harm. The defence of mistake of fact would be available by virtue of s 6.1 of the *Criminal Code.* This defence would have been available where an officer considered whether or not certain facts existed—for example, facts that would make the disclosure harmless—at or before the time of the disclosure, and was under a mistaken but reasonable belief about those facts, and had those facts existed, the conduct would not have constituted an offence.

6.116 The ALRC proposed this strict liability approach to the requirement to prove harm on the basis that Commonwealth officers have access to Commonwealth information because they hold positions of trust in the community. Such positions involve a level of responsibility to take care that information that could potentially harm essential public interests is not disclosed without authority. The approach was consistent with the ALRC's previous recommendation in its report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* that secrecy provisions should apply only to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.[112]

Submissions and consultations

6.117 A number of stakeholders expressed support for the concept of a tiered general secrecy offence 'where the evidentiary burden on the prosecution increases commensurate with the level of harm and penalty imposed'.[113] For example, Civil Liberties Australia (CLA) stated that:

---

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

113 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

> this approach introduces proportionality, consistency and gives better guidance to the courts and Commonwealth officers. We believe that this model ensures that the penalty fits with other penalties in Commonwealth law.[114]

6.118 There was very little support, however, for the ALRC's proposed first tier, strict liability offence. In response to IP 34, the AGD noted that evidential difficulties usually arise in relation to fault elements applicable to circumstances or results, and submitted that:

> 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:
>
> - 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.[115]

6.119 The AGD suggested that an objective test—such as that used in reg 2.1 of the *Public Service Regulations*, that an APS employee must not disclose information where it is reasonably foreseeable that the disclosure would be prejudicial to the effecting working of government—would be the preferred approach in relation to the requirement to prove harm.[116]

6.120 In response to DP 74, the AGD noted the policy position put in the *Guide to Framing Commonwealth Offences* that strict liability should not normally apply to an element of an offence where the penalty includes imprisonment or where there is a monetary penalty greater than 60 penalty units. The AGD suggested that the ALRC consider whether there were sufficient grounds to depart from the *Guide* in this case:

> The application of strict liability may unfairly subject people who have disclosed information to punishment for unforeseen consequences. If the proposed penalty remains, consideration might be given to including an additional element similar to that in s 58 of the *Defence Force Discipline Act*: that the disclosure was made without authorisation. The fault element of recklessness could apply to this element. This would help to ensure sufficient safeguards against the unfair prosecution of an individual who unwittingly commits the offence.[117]

6.121 The AGD noted the proposed exception to the general offence where the disclosure was authorised by the minister or agency head, and that the 'authorised by law' defence at section 10.5 of the *Criminal Code* would also apply. While suggesting

---

114 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
115 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
116 Ibid.
117 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

this may have substantially the same effect as an element stating that the disclosure was made without authorisation, the AGD's view was that it may be preferable for the prosecution to have to positively prove that the disclosure was not authorised.[118]

6.122 The Department of Defence stated that:

> the offence created by section 58 of the *Defence Force Discipline Act* indicates that the unauthorised disclosure, by members of the ADF and defence civilians, of information that is likely to be prejudicial to the security or defence of Australia is unacceptable. Defence would note that it is solely the seriousness of the harm, described in paragraph 58(1)(c) within the military context, that justifies the application of strict liability to that element of the offence.[119]

6.123 CLA did not support the use of strict liability in relation to the harm requirement, and expressed the view that criminal sanctions should only be imposed where there is an intention to cause harm, or recklessness as to harm. A number of other stakeholders agreed.[120]

6.124 CLA stated, however, that if the ALRC were to recommend an offence provision in which strict liability attached to the harm requirement, then a defence modelled on s 58 of the *Defence Force Discipline Act*—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—should be available.[121] Liberty Victoria expressed similar views.[122]

6.125 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 automatic fault elements set out in the *Criminal Code*.[123]

ALRC's views

6.126 The ALRC has reconsidered the proposal to have a tiered general secrecy offence and, in particular, the proposal to attach strict liability to the harm element of the first tier offence. The ALRC remains of the view that Commonwealth officers hold positions of trust in the community that attract a high level of responsibility in relation to information that could potentially harm specified essential public interests such as national security and defence.

---

118 Ibid.
119 Department of Defence, *Submission SR 69,* 14 August 2009.
120 Australia's Right to Know, *Submission SR 72,* 17 August 2009; Australian Press Council, *Submission SR 62,* 12 August 2009; Liberty Victoria, *Submission SR 19,* 18 February 2009; Australian Press Council, *Submission SR 16,* 18 February 2009.
121 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
122 Liberty Victoria, *Submission SR 50,* 5 August 2009.
123 The Treasury, *Submission SR 22,* 19 February 2009.

6.127 However, the ALRC recognises that the requirement for a fault element is one of the most fundamental protections of the criminal law and has decided that, on balance, the general secrecy offence should be limited to the unauthorised disclosure of Commonwealth information by a Commonwealth officer who knows, intends, or is reckless as to whether, the disclosure will harm, or is reasonably likely to harm, one of the public interests set out in Recommendation 5–1.

Recommendation 6–5 The general secrecy offence should require that a Commonwealth officer knew, intended that, or was reckless as to whether, the disclosure of Commonwealth information would harm, or was reasonably likely to harm, one of the public interests set out in Recommendation 5–1.

Initial and subsequent disclosures

6.128 Most secrecy provisions regulate the initial unauthorised disclosure of Commonwealth information. As McGinness has noted, however, this can give rise to problems:

> 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.[124]

6.129 As noted in Chapter 3, a number of existing secrecy provisions regulate both the initial disclosure, whether authorised or unauthorised, and any subsequent unauthorised disclosure of Commonwealth information. For example, s 8XB(1) of the *Taxation Administration Act* provides in part that a person shall not use or disclose taxation information that the person has obtained in breach of a provision of a taxation law. Section 8XB(2) provides that:

> Without limiting subsection (1), a person shall be taken to have obtained taxation information in breach of a provision of a taxation law if:
>
> (a) the information relates to the affairs of another person;
>
> (b) the form or circumstances in which the information was obtained would have led a reasonable person to believe that:
>
> (i) in the case of information contained in a document—the document had come from an office of the Commissioner or a Deputy Commissioner; or
>
> (ii) in any other case—the information had come from the records of the Commissioner or from an officer; and

124 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 64.

> (c) the information was obtained by the person in circumstances that gave the person no reasonable cause to believe that the communication of the information to the person was authorised by a taxation law or by a person acting in accordance with such a law.

6.130 The Tax Laws Exposure Draft Bill proposes to regulate both initial and subsequent disclosures through three separate offences to address:

- 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.[125]

6.131 The proposed taxation provisions stipulate that an individual does not commit an offence if the information was obtained with authority—that is, under one of the disclosure exceptions—and the information is subsequently disclosed for, or in connection with, the original purpose of disclosure.[126] However, an offence is committed where the subsequent disclosure does not fall within one of the exceptions to the prohibition on disclosure.[127] The following example is provided in the Explanatory Material:

> 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.[128]

6.132 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;

---

125 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.9].

126 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-155.

127 Ibid.

128 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.32].

> (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 ...

6.133 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 recommends that, in some circumstances, the subsequent disclosure of Commonwealth information by any person who receives the information in confidence or knowing, or reckless as to whether, the information has been disclosed in breach of the general secrecy offence should also be an offence.[129]

6.134 The Franks Committee expressed the view that:

> Our general approach has been to identify that official information which requires protection because it is genuinely secret. Whoever lets out such a secret, the same damage is done to the nation. Every citizen who knowingly handles a secret of this kind ought to protect it. If a civil servant has failed to protect a secret, there is no justification for the view that a citizen who thereby comes into possession of that secret, and who knows that it is a secret, should be free to compound the failure of the civil servant, and to harm the nation, by passing on the secret as he pleases.[130]

6.135 The Committee noted that while public servants have a clear public duty to safeguard official information, others are not subject to the same duty. Thus, others should not be subject to criminal sanctions unless they are aware that they have come into possession of secret information or the circumstances are such that they should clearly be aware of this:

> If the citizen knows that he is in possession of a secret but chooses nevertheless to disclose it, it is then reasonable that he should be liable to criminal penalties. The imposition of legal liability on the citizen is equitable, as well as being necessary for the protection of the nation on two conditions. The first is that the law should be strictly confined to what is genuinely secret. The second is that it should clearly specify that the citizen must be proved to have had guilty knowledge.[131]

---

129 Recommendations 6–6, 6–7.

130 Departmental Committee on Section 2 of the Official Secrets Act 1911, *Report of the Committee*, Vol 1 (1972), 85.

131 Ibid, 86.

6.136 The *Official Secrets Act 1989* (UK) includes a provision prohibiting the disclosure of information that has come into a person's possession as the result of an unauthorised disclosure, or where it has been entrusted to the person 'on terms requiring it to be held in confidence'. In order to commit the offence the person must know, or have reasonable grounds to believe, that the information is protected by the provisions of the Act and that it has come into his or her possession in the circumstances set out above.[132]

6.137 When Commonwealth information is disclosed by a third party without authority, the action for breach of confidence may provide a remedy. An action for breach of confidence can be brought against a third party who has received confidential information. The information may have been communicated in breach of a duty of confidence,[133] or may have come into the hands of the third party by human error.[134] 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.[135]

6.138 While an action for breach of confidence may provide some protection for confidential information, in 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs report, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth*, expressed the view that secrecy offence provisions should prohibit unauthorised dealing in confidential third party information at every point in the 'distribution chain', where there was the requisite mental element.[136]

6.139 The earlier *Review of the Commonwealth Criminal Law*, by a committee chaired by Sir Harry Gibbs (the Gibbs Committee), recommended that Australian legislation should follow the model provided by the UK *Official Secrets Act*, 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

---

132 *Official Secrets Act 1989* (UK) s 5.

133 See, eg, *Commonwealth v Fairfax* (1980) 147 CLR 39, 50–51 in which 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.

134 See, eg, *Victoria v Nine Network* (2007) 19 VR 476.

135 The equitable action for breach of confidence in relation to Commonwealth information is discussed in Ch 3.

136 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].

> (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.[137]

6.140 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.[138] 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.[139]

6.141 In DP 74, the ALRC proposed that unauthorised disclosure by current and former Commonwealth officers be covered by the general secrecy offence, which applied to all Commonwealth officers, including Commonwealth contracted service providers. Thus, all disclosures between Commonwealth agencies, and between agencies and their contractors, were to be covered by the general secrecy offence. The proposed subsequent disclosure offence was to cover unauthorised disclosures by other people where:

- information was disclosed by a Commonwealth officer in breach of the proposed general secrecy offence;
- the person knew, or was reckless as to whether, the information had been disclosed in breach of the proposed general secrecy offence; and
- the person knew, intended, or was reckless as to whether, the subsequent disclosure of the information would harm, or was reasonably likely to harm, one of the public interests protected by the general secrecy offence.[140]

6.142 The ALRC did not propose an offence to cover unauthorised disclosure of information by individuals who receive the information as a result of a lawful

---

137 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 333.

138 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 3–5.

139 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009; Australian Federal Police, *Submission SR 33,* 3 March 2009; Department of Human Services, *Submission SR 26,* 20 February 2009; The Treasury, *Submission SR 22,* 19 February 2009; Australian Commission for Law Enforcement Integrity, *Submission SR 18,* 18 February 2009; Australian Taxation Office, *Submission SR 13,* 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.

140 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 8–3.

disclosure, although the ALRC did seek stakeholder views on this issue. The ALRC's preliminary view was that, 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 a private sector organisation—the Commonwealth has the opportunity to ensure that appropriate safeguards are in place, or are put in place, to protect the information. For example, state and territory officers are usually subject to state and territory secrecy provisions,[141] or specific Commonwealth secrecy provisions. Intergovernmental or inter-agency agreements or contractual arrangements could be put in place 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.[142]

Submissions and consultations

Support for the subsequent disclosure offence

6.143 In response to IP 34, the AGD submitted 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.[143]

6.144 A number of stakeholders expressed broad support for a subsequent disclosure offence.[144] The AIC was also supportive, noting that if the proposed offence did not go ahead in relation to the general secrecy offence:

> the AIC submits that a subsequent disclosure offence should be added to the ASIO Act and the [*Intelligence Services Act*] and to any new secrecy offences relevant to ONA and DIO due to the serious harm caused by subsequent disclosure of AIC information.[145]

---

141 State and territory secrecy provisions are discussed in Chs 3 and 13.

142 The equitable action for breach of confidence is discussed in Ch 3.

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

144 Department of Human Services, *Submission SR 83,* 8 September 2009; Australian Privacy Foundation, *Submission SR 71,* 16 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009; Australian Federal Police, *Submission SR 33,* 3 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.

145 Australian Intelligence Community, *Submission SR 77,* 20 August 2009.

6.145 The ATO's view was that 'it is critical that information which has been disclosed in breach of a secrecy provision remains confidential'. The ATO expressed concern, however, that the requirement that the person know, intend, or be reckless as to whether the subsequent disclosure would cause harm would limit the utility of the proposed offence.[146]

6.146 The Treasury expressed support for the proposal to create an offence for subsequent disclosure noting that the Tax Laws Exposure Draft Bill regulates the subsequent disclosure of information obtained lawfully, as well as unlawfully. The Treasury commented that this was possible and desirable in the taxation context because the Tax Laws Exposure Draft Bill clearly identifies the circumstances in which tax information may be disclosed, usually in terms of the agency to which information can be disclosed and the purpose for which the information may be disclosed:

> Given that these disclosures are limited to particular purposes, there would be an understandable expectation that these limitations would continue to apply. Otherwise the initial limitations on disclosure by the ATO would arguably be of little importance.[147]

6.147 The Treasury suggested, however, that this rationale may not apply to the general secrecy offence:

> The Tax Secrecy Bill proposes to impose limitations on the on-disclosure of taxpayer information by clearly distinguishing between 'tax officers' and 'non taxation officers' who are in receipt of information lawfully. In the general context, imposing limitations on 'non-Commonwealth officers' might have limited effect given most lawful disclosures would likely occur between Commonwealth agencies. In relation to disclosures to non-Commonwealth officers, as the discussion paper notes, this may be more usefully addressed through agreements or, as in the case of the proposed Tax Secrecy Bill, through agency specific secrecy provisions.[148]

6.148 A number of other agencies, however, submitted that the subsequent disclosure offence should cover subsequent unauthorised disclosures of information that was initially disclosed lawfully.[149] The AIC expressed support for the Gibbs Committee recommendations and suggested that the offence should cover unauthorised disclosure of information by a person where the information has been entrusted to that person in confidence.[150]

6.149 The AGD drew attention to the increased need to share information with parties outside the Australian Government such as state and territory governments and the private sector and stated that the current reliance on state and territory secrecy

---

146 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
147 The Treasury, *Submission SR 60,* 10 August 2009.
148 Ibid.
149 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009; Australian Federal Police, *Submission SR 70,* 14 August 2009.
150 Australian Intelligence Community, *Submission SR 77,* 20 August 2009.

provisions and administrative arrangements did not provide a consistent level of protection for Commonwealth information. The AGD also considered that it was not sufficient to rely on commercial arrangements with the private sector. The AGD was firmly of the view that the proposed offence provisions should cover unauthorised disclosures of information received 'lawfully from a Commonwealth officer for a specified purpose':

> Without this, there will be no protection provided to Commonwealth information under the proposed general secrecy offence where the information was on-disclosed by an individual not covered by the definition of Commonwealth officer. …
>
> The terms of reference for this inquiry note the desirability of having comprehensive, consistent and workable laws and practices in relation to the protection of Commonwealth information. A general secrecy offence regulating the disclosure of Commonwealth information regardless of where that disclosure occurs or who discloses that information would provide certainty for those disclosing and receiving information. This approach would also achieve a level of uniformity in the protection of Commonwealth information nationally.[151]

Opposition to the subsequent disclosure offence

6.150 CLA did not support the proposed subsequent disclosure offence:

> CLA disagrees with the ALRC's view that 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, that it is reasonable to impose criminal sanctions for subsequent disclosure.[152]

6.151 CLA noted that the legislative, administrative and employment obligations imposed on Commonwealth officers are different to the responsibilities of journalists. In CLA's view it would be inappropriate to impose on journalists sanctions similar to those imposed on public servants, because journalists are not subject to the same obligations. In addition, CLA stated that the proposed provision would unreasonably limit journalists' discretion.[153]

6.152 The Australian Press Council agreed, stating that:

> The Council is particularly concerned with the impact of the proposed subsequent disclosure offence on media professionals. The importance of a public interest defence in such matters is paramount. Whether or not comprehensive public interest disclosure legislation is eventually approved by the Parliament, the Council submits that a public interest defence needs to be an integral part of the proposed subsequent disclosure offence.[154]

---

151 Attorney-General's Department, *Submission SR 67,* 14 August 2009.
152 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
153 Ibid.
154 Australian Press Council, *Submission SR 62,* 12 August 2009.

6.153 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':

> 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.[155]

6.154 The Press Council suggested that secrecy provisions should expressly provide for unauthorised disclosures to journalists. It 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 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.[156]

6.155 Other stakeholders also expressed concern about the proposed subsequent disclosure offence,[157] particularly in the absence of a robust whistleblower regime.[158]

ALRC's views

6.156 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.[159] The second and third of these proposed offences endeavour to deal with the subsequent unauthorised disclosure of taxation information.

---

155 Australian Press Council, *Submission SR 16,* 18 February 2009.
156 Ibid.
157 Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009; L McNamara, *Submission SR 51,* 6 August 2009.
158 L McNamara, *Submission SR 51,* 6 August 2009.
159 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [3.9].

6.157 Although most existing secrecy provisions do not seek to address subsequent unauthorised disclosures, the ALRC sees merit in subsequent disclosure offence provisions in two limited circumstances.

6.158 First, the ALRC recommends that a subsequent disclosure offence should apply 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 discloses that information knowing, intending, or reckless as to whether, the disclosure would harm one of the essential public interests identified in Chapter 5.

6.159 In DP 74, the ALRC did not propose to cover unauthorised disclosure of information by individuals who receive the information as a result of a lawful disclosure. This was on the basis that, because the initial disclosure was with authority, the Australian Government maintained control of the disclosure and would have the opportunity to ensure that appropriate safeguards were in place, or were put in place, to protect the information.

6.160 A number of stakeholders were firmly of the view, however, that these mechanisms did not provide adequate protection.[160] They suggested that there should also be a criminal offence where Commonwealth information is disclosed to a person for a specified purpose, or in confidence, and that person discloses it for an unrelated and unauthorised purpose, knowing or reckless as to whether the disclosure will, or is likely to, cause harm.

6.161 The ALRC is concerned that basing this subsequent disclosure offence on the fact that information is disclosed for a specified purpose may create uncertainty. In the taxation context, taxation information may only be disclosed to specific parties and for specific purposes, and so it is possible to draft a subsequent disclosure offence with sufficient clarity to prohibit the disclosure of taxation information except 'for the original purpose or in connection with the original purpose'.[161] This is not possible in the context of the general secrecy offence and subsequent disclosure offences because the provisions apply to all Commonwealth information, and the circumstances in which such information may be disclosed are not defined in the same way.

6.162 The ALRC recommends, therefore, that the second subsequent disclosure offence be based on the model provided by the UK *Official Secrets Act* and recommended by the Gibbs Committee. This offence would be committed where Commonwealth information is disclosed to a person who is not a Commonwealth

---

160 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Australian Intelligence Community, *Submission SR 77,* 20 August 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009; Australian Federal Police, *Submission SR 70,* 14 August 2009; Attorney-General's Department, *Submission SR 67,* 14 August 2009.

161 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-175.

officer, on terms requiring it to be held in confidence, and that person discloses the information in breach of those terms knowing, intending, or reckless as to whether, the disclosure will, or is reasonably likely to, harm one of the specified public interests. As noted in Chapter 3, an obligation to hold information in confidence may arise in a number of ways, for example, on the basis of the circumstances in which the information is disclosed, or because of an express contractual stipulation.

6.163 This offence will cover some conduct currently covered by s 79 of the *Crimes Act*, that is, the unauthorised disclosure of information 'entrusted to a person by a Commonwealth officer or a person holding office under the Queen' and 'by reason of the its nature or the circumstances under which it was entrusted to him or her … it is his or her duty to treat it as a secret'. Section 79(3), for example, makes it an offence to disclose such information without a duty or the authority to disclose it. The recommended subsequent disclosure offence is, however, limited to disclosures that are likely to harm an essential public interest.

6.164 It is the ALRC's view that it would not be appropriate to provide an exception from criminal liability under the subsequent disclosure offences for the media where the disclosure is intentional and there is the requisite fault element in relation to the potential harm. Both the initial and subsequent disclosure offences are framed to indicate the circumstances in which disclosure is clearly not in the public interest. Those circumstances are defined and limited to protect only essential public interests, where the unauthorised disclosure will, or is reasonably likely to, have very serious consequences. In the ALRC's view, the intentional and unauthorised disclosure of such information warrants criminal sanctions.

6.165 In the ALRC's view it would not be appropriate to criminalise the mere receipt of Commonwealth information in the subsequent disclosure offences—even where the information has been disclosed in contravention of the general secrecy offence—if there is no subsequent disclosure. Those who receive such information should have the opportunity to take appropriate action, for example, to inform the relevant agency.

6.166 The proposed subsequent disclosure offences should be subject to a number of exceptions and defences. These are discussed in detail in Chapter 7. Chapter 2 considers the Australian Government's proposal to develop public interest disclosure legislation. It will be important to ensure that, under the proposed legislation, where a Commonwealth officer makes a public interest disclosure in accordance with public interest disclosure legislation—and is therefore protected from criminal liability under any relevant secrecy offence, including the recommended general secrecy offence—the subsequent disclosure of the information by a non-Commonwealth officer is also protected. This issue is discussed further in Chapter 7.

Recommendation 6–6 There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) in breach of the general secrecy offence; and

(b) B knows, or is reckless as to whether, the information has been disclosed in breach of the general secrecy offence; and

(c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.

Recommendation 6–7 There should be a new offence in the *Criminal Code* (Cth) for the subsequent unauthorised disclosure of Commonwealth information where:

(a) the information has been disclosed by Commonwealth officer A to B (not a Commonwealth officer) on terms requiring it to be held in confidence;

(b) B knows, or is reckless as to whether, the information has been disclosed on terms requiring it to be held in confidence; and

(c) B knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—one of the public interests set out in Recommendation 5–1.

7. General Secrecy Offence: Exceptions and Penalties

Contents

Introduction

7.1 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 an 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 considers which exceptions or defences should be included in the ALRC's recommended general secrecy offence and

subsequent disclosure offences.[1] It will also consider the interaction of these offences with public interest disclosure legislation proposed by the House of Representatives Standing Committee on Legal and Constitutional Affairs and discussed in Chapter 2.[2] Finally, the chapter considers the penalties that should apply for breach of the general secrecy offence and the subsequent disclosure offences.

Exceptions and defences

7.2 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 to excuse conduct that is prohibited by a secrecy offence.

7.3 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.

7.4 In some circumstances, the distinction between an exception and a defence will be of limited significance. 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 burden in relation to that matter'.[3] The *Criminal Code* also provides that, except in particular circumstances, or where an offence expressly provides otherwise, where a burden of proof is imposed on a defendant, it is an evidential burden only.[4]

7.5 An evidential burden requires a defendant to provide evidence that suggests a reasonable possibility that the exception or defence is made out.[5] Once the defendant has met the evidential burden, the prosecution must refute the exception or defence and prove all elements of the offence beyond reasonable doubt.[6]

---

1 Recommendations 5–1, 6–6, 6–7.

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

3 *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).

4 *Criminal Code* (Cth) s 13.4.

5 Ibid s 13.3.

6 Ibid s 13 1.

7.6 While framing a provision as a defence, rather than as an exception, does not of itself alter evidential burdens of proof, it may have procedural disadvantages for a defendant, in that a defendant must wait until the defence case is called before being able to lead evidence to justify his or her conduct.

7.7 Some offences expressly impose a legal burden of proof on the defendant.[7] A legal burden requires the defendant to establish the exception or defence on the balance of probabilities. Once this is done, the prosecution must refute the exception or defence beyond reasonable doubt.[8]

7.8 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:

> 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.[9]

7.9 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 been considered, in itself, a sound justification for taking the significant step of reversing the onus of proof.[10]

Defences available under the *Criminal Code*

7.10 The *Criminal Code* 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 to these as 'defences', although the *Code* does not characterise them in this way.[11] 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);

---

7 Ibid s 13.4. See, eg, *Crimes Act 1914* (Cth) s 79(5) and (6) for examples of secrecy offences in which the defendant bears a legal burden of proof. A legal burden of proof is created when the offence expressly provides that there is a legal burden of proof on the defendant, or requires the defendant to 'prove' the matter.

8 *Criminal Code* (Cth) s 13.5.

9 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 28–29.

10 Ibid, 28.

11 Part 2.3 of the *Criminal Code* (Cth) is headed 'Circumstances in which there is no criminal responsibility'.

- duress (s 10.2);
- sudden or extraordinary emergency (s 10.3); and
- conduct justified or excused by or under a law (s 10.5).

7.11 In its submission, the AGD noted that these provisions were intended to codify the general defences available at common law.[12] 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.[13]

Which exceptions and defences should be expressly included?

7.12 Chapter 3 identifies a range of exceptions and defences found in existing secrecy provisions, that is, where disclosure is

- in the course of a person's functions and duties;
- for the purposes of a particular law;
- authorised by specified persons;
- to specified persons or entities;
- for the purposes of legal proceedings;
- for the purposes of law enforcement;
- with consent;
- of de-identified information;
- to avert threats to life or health; and
- in the public interest.

7.13 In response to the Issues Paper, *Review of Secrecy Laws* (IP 34),[14] 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

12 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
13 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 27.
14 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).

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.[15]

7.14 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC proposed that the general secrecy offence should expressly include exceptions or defences where 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.[16]

7.15 In this section, the ALRC considers stakeholder response to this proposal and examines how the defences in the *Criminal Code* would operate in relation to the general secrecy offence.

In the course of an officer's functions and duties

7.16 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.[17]

7.17 The 'performance of duties' exception has been interpreted widely to govern all that is incidental to carrying out the functions and duties authorised by an officer's employment.[18] However, the Australian Government Solicitor has advised that the duties authorised by an officer's employment extend only to those duties that have some basis in the legislation governing the officer, such as legislation administered by the employing agency or the *Public Service Act 1999* (Cth).[19]

---

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

16 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–1.

17 *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2).

18 *Canadian Pacific Tobacco Co Ltd v Stapleton* (1952) 86 CLR 1, 6.

19 D Boucher, *Report of a Review of Information Handling Practices in the Serious Non Compliance Business Line of the Australian Taxation Office* (2008), Attachment 9.

7.18 The Treasury's review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review) noted that the meaning of disclosure in the 'course of duties of an officer' is uncertain and should be clarified.[20] Issues have arisen in the taxation context in relation to the release of information by taxation officers for the purposes of another agency, for example, a law enforcement agency. 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.[21]

7.19 The Tax Laws Exposure Draft Bill, like a number of existing specific 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.[22] Some of these are quite general—for example, 'for the purpose of administering a taxation law',[23] or 'for the purpose of criminal, civil or administrative proceedings (including merits review or judicial review) that are related to a taxation law'.[24] 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'.[25]

7.20 The specific secrecy provisions regulating the activity of the Australian Securities and Investments Commission (ASIC), the Australian Prudential Regulation Authority (APRA), and the Australian Bureau of Statistics are also in the form of a general prohibition on disclosure, followed by a list of situations in which disclosure is authorised.[26] For example, s 127 of the *Australian Securities and Investments Commission Act 2001* (Cth) (ASIC Act) 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, staff member or ASIC delegate.

---

20 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 19.

21 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.6].

22 Ibid, [5.8].

23 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-45(2) table item 1.

24 Ibid sch 1 pt 1 cl 355-45(2) table item 3.

25 Ibid sch 1 pt 1 cl 355-45 table item 5.

26 *Australian Securities and Investments Commission Act 2001* (Cth) s 127; *Australian Prudential Regulation Authority Act 1998* (Cth) s 56; *Census and Statistics Act 1905* (Cth) s 19.

7.21 In DP 74, the ALRC proposed that the general secrecy offence should provide an exception for disclosures in the course of a Commonwealth officer's functions or duties.[27] The ALRC considers that it would not be possible for the general secrecy offence to include a list of authorised disclosures because the offence covers all Commonwealth officers and all Commonwealth information. The ALRC expressed the view that it would be possible to clarify the scope of the proposed exception through the legislation governing particular agencies, agency guidelines or inter-agency memorandums of understanding (MOUs).

Submissions and consultations

7.22 The ATO submitted that a general exception permitting disclosures in the performance of an officer's duties was 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.[28]

7.23 The ATO noted that the phrase 'in the performance of duties' has had significant judicial consideration which has assisted the ATO in determining the scope of the exception:

> In some limited circumstances there will be uncertainty about whether a particular disclosure will be permitted by this exception. However, it is our experience that generally whether a disclosure is within the performance of an officer's duties is capable of ascertainment. In addition, the performance of duties exception is read with reference to its legislative background; in the tax context, by reference to those duties which are related to or connected to the performance of a person's duties as an officer.[29]

7.24 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.[30]

7.25 ASIC submitted that the specific circumstances in which disclosures should be permitted must be determined by reference to the functions and duties of each Commonwealth agency. ASIC noted that where secrecy provisions attempt to list authorised disclosures—as in s 127 of the ASIC Act—it is important to ensure that the

---

27 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–1(a).

28 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

29 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

30 The Treasury, *Submission SR 60,* 10 August 2009; The Treasury, *Submission SR 22,* 19 February 2009.

list is inclusive, rather than exhaustive, and suggested that s 127 of the ASIC Act may be an appropriate model.[31]

7.26 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.[32] Some stakeholders were also concerned that the exception may be too broad and create uncertainty.[33] The Australian Transaction Reports and Analysis Centre (AUSTRAC) considered that attempting to define the limits of the exception in agency guidelines or inter-agency MOUs 'would be problematic as they would not be legally binding and would need to be job specific'. Instead, AUSTRAC suggested that the exception in the general secrecy offence would need to be supported by specific secrecy provisions that define the ambit of those functions and duties.[34]

7.27 On the other hand, 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.[35]

ALRC's views

7.28 In the ALRC's view, it is essential to include an exception in the general secrecy offence for disclosure in the course of an officer's functions or duties. Although detailed lists of authorised disclosures may be included in specific secrecy provisions governing the activities of specific agencies, this will not be possible in the general secrecy offence. This is because the provision is intended to apply across all agencies and all Commonwealth information. It is, however, possible to provide clarity about the scope of the exception in other ways.

7.29 For example, 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 general secrecy offence.[36] 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

---

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

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

33 Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

34 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

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

36 Such disclosures may also fall within the 'conduct justified or excused by or under law' exception, discussed below. The interaction between the general secrecy offence and specific secrecy offences is discussed further in Ch 10.

remove the prohibition—while leaving the list of authorised disclosures in place—and rely, instead, on the general secrecy offence.[37]

7.30 Most agencies are not, however, governed by legislation that includes detailed information-sharing regimes. In these circumstances the framework for an officer's duties and functions will be set by more general instruments, for example the *Public Service Act* in relation to Australian Public Service (APS) employees, or contractual terms for contracted service providers.

7.31 Within the boundaries set by these framework instruments, it is possible to indicate in more detail those disclosures that fall within an officer's functions and duties by issuing agency policies and guidelines or inter-agency MOUs dealing with information sharing. As discussed in Chapter 14, the Australian Public Service Commission advises that agencies should 'establish clear policies and guidelines so that employees are aware of the provisions that govern the management of information'.[38] Any such policies, guidelines or MOUs must, however, be consistent with the legislative framework.

On the authority of specified persons

7.32 Chapter 3 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,[39] or other persons, including agency heads[40] or the responsible minister.[41] A number of these provisions require the authorising person to certify that the disclosure is necessary in the public interest.

7.33 For example, s 86-3 of the *Aged Care Act 1997* (Cth) provides that the Secretary of the Department of Health and Ageing (DoHA) 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.[42]

7.34 In the administrative context, reg 2.1 of the *Public Service Regulations 1999* (Cth) provides that a disclosure is allowed if the information is disclosed in accordance with an authorisation given by an agency head.[43] As discussed in Chapter 13, similar

---

37 This issue is discussed further in Ch 4.

38 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009, Ch 3.

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 The *Public Service Act 1999* (Cth) defines agency head to mean the secretary of a department, the head of an executive agency, or the head of a statutory agency: s 7.

exceptions exist in some states and territories, for example, s 57 of the *Public Sector Management Act 1995* (SA) allows disclosures of official information where they are 'made with the permission of the Chief Executive of the administrative unit in which the employee is employed'.

7.35 In DP 74 the ALRC proposed that the general secrecy offence should be subject to an exception where the disclosure is authorised by the relevant agency head or minister, and the agency head or minister certifies that the disclosure is in the public interest.[44]

Submissions and consultations

7.36 A number of stakeholders expressed concern about the breadth of the proposed exception. DoHA, for example, noted that the proposed exception was broader than those in the *Aged Care Act* and the *Health Insurance Act*, which are limited to disclosures 'necessary in the public interest'.[45]

7.37 The ATO submitted that, in the taxation context, 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 and would potentially allow the disclosure of information damaging to individuals or corporations.[46] The Treasury noted that the Taxation Secrecy Review also considered, and did not pursue, a broad discretion for the Commissioner of Taxation to authorise disclosures. The Treasury 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.[47]

7.38 The Australian Privacy Foundation was concerned that the exception proposed was too broad, and queried whether the authorisation would have to be made in advance and in writing. The Foundation also expressed the view that an unlimited ad hoc ability to authorise disclosures was objectionable and should at least be subject to objective public interest criteria, adequate controls and reporting requirements to prevent abuse.[48]

7.39 Civil Liberties Australia (CLA) expressed support for the proposed exception.[49] The AGD agreed, stating that, while completely codifying the circumstances in which

---

44 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–1(b).

45 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.

46 Australian Taxation Office, *Submission SR 55,* 7 August 2009; Australian Taxation Office, *Submission SR 13,* 16 February 2009.

47 The Treasury, *Submission SR 60,* 10 August 2009; The Treasury, *Submission SR 22,* 19 February 2009.

48 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

49 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

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.[50]

ALRC's views

7.40 An exception for disclosures authorised by an agency head or minister may not be appropriate in specific secrecy provisions, such as the taxation provisions, where the provision sets out a comprehensive list of authorised disclosures. In the ALRC's view, however, an exception of this kind is necessary in the context of the general secrecy offence. The general secrecy offence is intended to apply to all Commonwealth officers and all Commonwealth information and does not include a comprehensive list of authorised disclosures. In these circumstances, it is necessary to ensure that the provision is flexible enough to meet the operational requirements of government.

7.41 In Chapter 5, the ALRC recommends 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.[51] However, circumstance may arise where disclosure will be in the overall public interest, despite the potential harm. 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, on balance, it would be in the public interest to disclose the information in order to protect public health or safety.

7.42 Because the information protected by the general secrecy offence has the potential to cause serious harm, 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 before the information is disclosed.

7.43 Decisions of an agency head or minister to authorise disclosure in the public interest will not be unlimited or unconstrained. In construing the scope of the exception, the subject matter and purpose of the secrecy offence will be relevant.[52] In addition, administrative law principles require, for example, that the agency head or minister exercise his or her discretion for an authorised purpose and that any decision must be reasonable and made in good faith.

---

50 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
51 Recommendation 5–1.
52 *Acts Interpretation Act 1901* (Cth) s 15AA.

7.44 The exception is intended to introduce an element of flexibility into the offence regime—for example, where it is necessary to seek authorisation in an emergency. The ALRC is not, therefore, recommending that the authority must be in writing. However, the *APS Values and Code of Conduct in Practice* suggests that where APS employees seek advice because they are unsure about whether to disclose information, they should keep a record of that advice.[53]

7.45 The Exposure Draft Freedom of Information Amendment (Reform) Bill 2009 provides that an agency or minister must provide access to a document that is conditionally exempt, 'unless (in the circumstances) access to the document at that time would on balance, be contrary to the public interest'. The ALRC has adopted similar wording in the recommended exception to the general secrecy offence, that is, that it is an exception to the offence if the information was disclosed in accordance with an authorisation given by an agency head or minister that disclosure would, on balance, be in the public interest.

Information already in the public domain

7.46 Regulation 2.1(5) of the *Public Service Regulations* 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 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.[54]

7.47 The disclosure 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.[55]

---

53 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009, Ch 3.

54 Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006).

55 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 10–11.

7.48 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.[56]

7.49 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).

7.50 In DP 74, the ALRC proposed that the general secrecy offence and the subsequent disclosure offence should include exceptions where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.[57]

Submissions and consultations

7.51 A number of stakeholders expressed support for this proposal.[58] CLA was also supportive but submitted that the exception should not be limited to 'information that is already in the public domain as the result of a lawful disclosure' on the basis that it is irrelevant how the information came into the public domain.[59] Liberty Victoria agreed 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.

---

56 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.30].

57 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposals 8–4, 9–1(c).

58 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; The Treasury, *Submission SR 60,* 10 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009. See also: 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.

59 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

> As a result Liberty Victoria strongly supports an exception from penalty for disclosure of information already in the public domain.[60]

7.52 Some stakeholders cautioned, however, that it is sometimes difficult to establish whether information is in the public domain.[61]

7.53 The Commonwealth Director of Public Prosecutions (CDPP) noted that under the *Criminal Code*, if this exception was framed as suggested, the defendant would bear an 'evidential burden' in relation to whether information is in the public domain as the result of a lawful disclosure.[62] Once that burden is met by the defendant, the prosecution bears a legal burden to disprove the matter.[63] The CDPP stated that it may be difficult for the prosecution to disprove that information is in the public domain as the result of a lawful disclosure.[64]

7.54 Some stakeholders specifically commented on the inclusion of this exception in the subsequent disclosure offence. The ATO supported the inclusion of the proposed exception.[65] Liberty Victoria suggested, however, that it may be too limited:

> if the information is already in the public domain (whether legally or illegally) it may be difficult to attempt to restrict members of the public from repeating that disclosure. Liberty also believes that the ALRC's proposal may reduce certainty regarding the legality of subsequent disclosure in certain circumstances, for instance, where the precise circumstances (and the legality) of the initial disclosure may be unknown to the subsequent discloser.[66]

ALRC's views

7.55 As discussed in Chapter 5, the recommended general secrecy offence would impose criminal liability only where the disclosure 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 recommends, therefore, that the general secrecy offence should include an exception for disclosure of information in the public domain, but only where the information is *lawfully* in the public domain.

---

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

61 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Department of Human Services, *Submission SR 26,* 20 February 2009.

62 *Criminal Code* (Cth) s 13.3: As noted above, an evidential burden means 'the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist'.

63 Ibid s 13.1(2).

64 Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009.

65 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

66 Liberty Victoria, *Submission SR 50,* 5 August 2009.

7.56 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.[67]

7.57 In Chapter 6, the ALRC recommends two subsequent disclosure offences.[68] The first offence relates to information disclosed by a Commonwealth officer to a third party in breach of the general secrecy offence. The second relates to information disclosed by a Commonwealth officer to a third party on terms requiring it to be held in confidence.

7.58 In both these situations it is possible that the information will be lawfully put into the public domain after the Commonwealth officer has disclosed it to the relevant third party. In order to ensure that the third party is not subject to criminal sanctions for disclosing the information once it is lawfully in the public domain, both subsequent disclosure offences should include an exception in similar terms to the exception provided in the general secrecy offence.

7.59 For the reasons articulated above, this exception should also be limited to information that is in the public domain as the result of a lawful disclosure. Otherwise, a third party who has acquired Commonwealth information in breach of the general secrecy offence could rely on an earlier leak to justify publishing the information.

7.60 In relation to the burden of proof, the ALRC's view is that the defendant should bear an evidential burden in relation to this exception. That is, the defendant should be required to adduce or point to evidence that suggests a reasonable possibility that the information is in the public domain as the result of a lawful disclosure, for example, a press release or government report. The prosecution would then be required to refute the defence beyond reasonable doubt, that is, to prove that the information is in the public domain as a result of an unlawful disclosure, for example, that the press release was unauthorised, or fraudulent. This approach is reflected in s 91.2 of the *Criminal Code*, set out above.

Recommendation 7–1 The 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) in accordance with an authorisation given by an agency head or minister that the disclosure would, on balance, be in the public interest; or

67 *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413.
68 Recommendations 6–6, 6–7.

(c) of information that is already in the public domain as the result of a lawful disclosure.

Recommendation 7–2 The subsequent disclosure offences should include an exception where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.

Which exceptions and defences should not be expressly included?

Lawful authority

7.61 The *Criminal Code* includes a defence of 'lawful authority' where 'the conduct constituting the offence is justified or excused by or under a law'.[69] The *Commonwealth Criminal Code: A 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.[70]

7.62 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 disclosures 'for the purposes of the Act'—such as s 3C(2A) of the *Taxation Administration Act 1953* (Cth); and
- allow disclosures 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 *Corporations Act 2001* (Cth), *Payment Systems (Regulation) Act 1998* (Cth); *Payment Systems and Netting Act 1998* (Cth) and *Banking Act 1959* (Cth).

7.63 In its submission to this Inquiry, the 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.[71]

---

69 *Criminal Code* (Cth) s 10.5.

70 Australian Government Attorney-General's Department and the Australian Institute of Judicial Administration, *The Commonwealth Criminal Code: A Guide for Practitioners* (2002), 233.

71 Commonwealth Director of Public Prosecutions, *Submission SR 17,* 18 February 2009.

ALRC's views

7.64 Given the general application of the *Code* defence of lawful authority, it is not necessary to expressly include this defence in the general secrecy offence.

7.65 In Chapter 14, 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 prosecution.[72] It would be helpful to include a reference in any such policy to the 'lawful authority' defence.

7.66 In addition, the ALRC recommends 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 general secrecy offence and relevant exceptions and defences, including 'lawful authority'.[73]

7.67 Finally, the ALRC recommends that private sector organisations that perform services for or on behalf of the Australian Government under contract should ensure that all employees who have access to Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal or civil liability could result.[74] This should include reference to the obligations imposed by the new general secrecy offence and relevant exceptions and defences, including 'lawful authority'.

To specified persons or entities

7.68 As discussed in Chapter 3, a number of secrecy provisions provide exceptions to allow disclosures to specified persons or entities, such as ministers or government agencies.[75] These provisions are aimed at facilitating the legitimate sharing of information within government.

7.69 In other circumstances, provisions require that information must not be disclosed to specified persons—for example, to the minister. The Explanatory Material to the Tax Laws Exposure Draft Bill provides 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 laws and sensitivities associated with the possible release of taxpayer information into a public forum.[76]

---

72 Recommendation 14–1.
73 Recommendation 15–1.
74 Recommendation 13–4.
75 See, eg, *Environment Protection (Alligator Rivers Region) Act 1978* (Cth) s 31.
76 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.19].

7.70 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.[77]

Submissions and consultations

7.71 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.[78]

ALRC's views

7.72 The ALRC is not recommending the inclusion of a list in the general secrecy offence allowing disclosure to ministers or to other specified persons or entities. It is not possible to include this level of detail in a general offence applying to all Commonwealth officers and all Commonwealth information. These matters need to be considered at an individual agency level. Disclosures to ministers or other specific persons or entities that have been authorised, for example, in legislation, or under valid agency guidelines or inter-agency MOUs will fall within the exception in the general offence for disclosures in the course of an officer's functions or duties.

7.73 Where it is necessary to authorise or restrict disclosure of certain Commonwealth information to specified persons or entities, a specific secrecy provision can be used.

For the purposes of law enforcement

7.74 As discussed in Chapter 3, 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
>
> (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.

---

77 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 cl 355-55(1) table item 1.

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

7.75 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.[79] 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.[80]

7.76 The draft Bill also proposes to amend the provisions allowing disclosure to law enforcement agencies for the enforcement of 'serious criminal offences'.[81] 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 for prosecution.[82]

Submissions and consultations

7.77 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:

> 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.[83]

---

79 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 cl 355-65(1) table 3 item 1.

80 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.54].

81 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 cl 355-70 (1)(c)(i).

82 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.64].

83 Commonwealth Director of Public Prosecutions, *Submission SR 17,* 18 February 2009.

7.78 The ATO also noted that the existing taxation secrecy provisions inhibited its ability to share information with law enforcement agencies.[84] The Department of Education, Employment and Workplace Relations (DEEWR) 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.[85]

7.79 The Australian Federal Police and the CDPP expressed the view that the general secrecy offence should include an express exception for the exchange of information for law enforcement purposes.[86] The CDPP noted 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.[87]

7.80 The AGD's view was that, while the sharing of information with law enforcement agencies may come within one of the other proposed exceptions, there would be merit in having an express exception for disclosure to law enforcement agencies. The AGD suggested that an exception for providing information to law enforcement and regulatory agencies could include a threshold—for example, 'a Commonwealth officer may need to have a reasonable belief that the information is relevant to investigating a possible criminal offence or regulatory breach'.[88]

7.81 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.[89]

---

84 Australian Taxation Office, *Submission SR 13,* 16 February 2009.
85 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.
86 Australian Federal Police, *Submission SR 70,* 14 August 2009; Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009.
87 Commonwealth Director of Public Prosecutions, *Submission SR 17,* 18 February 2009.
88 Attorney-General's Department, *Submission SR 67,* 14 August 2009.
89 The Treasury, *Submission SR 22,* 19 February 2009.

ALRC's views

7.82 The ALRC recognises the importance of allowing information to flow to law enforcement and regulatory agencies in appropriate circumstances. However, the disclosure of Commonwealth information for the purposes of law enforcement is not always appropriate, and may need to be finessed. For example, as discussed above, the Tax Laws Exposure Draft Bill proposes to allow the disclosure of taxpayer information to law enforcement agencies only for the enforcement of *serious* criminal offences. Because of this, such disclosures should be regulated at an agency level, based on agency-specific legislation, agency policies and guidelines and inter-agency MOUs, rather than a blanket exception in the general secrecy offence. On this basis, such disclosures would fall within the recommended exception for disclosure in the course of an officer's duties and functions in the general offence.[90]

7.83 In addition, if it is not clear to a particular officer whether information should be passed on to a law enforcement agency, it would be possible, under the recommended general secrecy offence exceptions, to seek the agency head or minister's authority to disclose the information.[91]

For use in legal proceedings

7.84 A number of secrecy offences expressly regulate the disclosure of Commonwealth information to 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, where appropriate, such disclosures could generally 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 recommend that an exception for the disclosure of information for use in legal proceedings be included as an express exception in the general secrecy offence.

With consent

7.85 As discussed in Chapter 3, 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.[92]

7.86 In contrast, the Tax Laws Exposure Draft Bill does not include consent as a defence for an otherwise unauthorised disclosure.[93] 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

---

90 Recommendation 7–1(a).

91 Recommendation 7–1(b).

92 See, eg, *Gene Technology Act 2000* (Cth) s 187(1)(f); *Reserve Bank Act 1959* (Cth) s 79A(3); *National Health Act 1953* (Cth) s 135A(8).

93 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth).

> 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.[94]

Submissions and consultations

7.87 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.[95] A number of other agencies also expressed support for allowing disclosure with consent.[96] APRA noted that s 56 of the *Australian Prudential Regulation Authority Act 1998* (Cth) (APRA Act) allowed the release of personal information with the consent of the individual to whom the information relates.[97]

7.88 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.[98]

7.89 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.[99]

ALRC's views

7.90 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

---

94 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.15].

95 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

96 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.

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

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

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

ALRC is not recommending the inclusion of an exception for disclosure with consent in the new general secrecy offence.

7.91 Where it is desirable to allow release of information with consent, this should be made clear in agency-specific legislation or, so long as they are consistent with the relevant legislative framework, in 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.

A serious threat to a person's life, health or safety

7.92 As discussed in Chapter 3, 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.

7.93 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.[100] This exception reflects one of the exceptions in Information Privacy Principle 11 in the *Privacy Act 1988* (Cth)—which regulates the disclosure of personal information by Australian Government agencies.[101]

7.94 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.[102]

---

100 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 cl 355-90.

101 The Tax Laws Exposure Draft Bill provision does not include a requirement that the threat be imminent 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.

102 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.82]–[5.83].

7.95 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.

7.96 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.[103]

7.97 The *Commonwealth Criminal Code: A 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.[104]

7.98 The *Code* defence is a general defence that would be available in relation to the general secrecy offence and the subsequent disclosure offences.

Submissions and consultations

7.99 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.[105]

7.100 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

---

103 *Criminal Code* (Cth) s 10.3.

104 Australian Government Attorney-General's Department and the Australian Institute of Judicial Administration, *The Commonwealth Criminal Code: A Guide for Practitioners* (2002), 227.

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

> 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.[106]

7.101 DoHA was strongly of the view that the offence should include an express exception for disclosures necessary to prevent serious and imminent threats to life or health:

> For example, in the interests of protecting public health in a crisis such as the recent Victorian bushfires the Department believes that there is a need for provisions that allow competent authorities to exchange information that might otherwise be commercial-in-confidence to deal with the emergency.[107]

7.102 Whistleblowers Australia also expressed the view that the sudden or extraordinary emergency exception was not adequate to address the question of threats to life, health or safety.[108]

ALRC's views

7.103 In the ALRC's view, where a Commonwealth officer makes an unauthorised disclosure of Commonwealth information because it was necessary to prevent a serious and imminent threat to a person's life or health, the officer should not be subject to criminal sanctions.

7.104 However, where such a threat exists, there are a number of existing options to deal with the situation. First, where there is sufficient time to do so, it would be possible to seek authorisation from the relevant agency head or minister.[109] As noted above, such authorisations do not have to be in writing, to facilitate disclosures where necessary in an emergency. The general secrecy offence only relates to information that has the potential to cause serious harm, including for example, endangering someone's life. If there is sufficient time to consult an agency head or minister, and to consider the balance of interests involved at a senior level, this should be done.

7.105 In more extreme circumstances where there may not be time to seek permission for the disclosure, the *Criminal Code* defence of sudden or extraordinary emergency may be available. The defence would apply where a Commonwealth officer had a reasonable belief that a real threat exists—for example, the DHS example provided above where 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. Because the general

---

106 Department of Human Services, *Submission SR 26,* 20 February 2009.
107 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.
108 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.
109 Recommendation 7–1(b).

secrecy offence only relates to information that has the potential to cause serious harm if disclosed, in the ALRC's view, this defence provides an appropriate framework to allow disclosure in emergency situations, for example, where there is a serious and imminent threat to an individual's life.

A serious threat to public health or public safety

7.106 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.[110] 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.[111]

ALRC's views

7.107 The ALRC is not recommending 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.[112] The ALRC notes that such disclosures will sometimes fall within the 'sudden or extraordinary emergency' *Criminal Code* defence[113]—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.

7.108 For the purposes of this Report, the ALRC is proceeding on the basis that the Australian Government will enact public interest disclosure legislation, as proposed in the House of Representatives Standing Committee on Legal and Constitutional Affairs (Standing Committee) report, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (the *Whistleblower Protection* report).[114] In the report, discussed in detail in Chapter 2, 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, or other third parties, where the matter threatens immediate serious harm to public health or safety and has been disclosed to internal and external authorities, but

---

110 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 cl 355-90.

111 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [5.85].

112 Recommendation 7–1(b).

113 *Criminal Code* (Cth) s 10.3.

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

has not been acted on in a reasonable time.[115] A person who made such a disclosure under the proposed public interest disclosure legislation would be protected from criminal liability, including liability under the general secrecy offence.

Public interest disclosure

Public interest exceptions in secrecy provisions

7.109 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',[116] the meaning and scope of this exception is unclear.[117]

7.110 As noted in Chapter 3, 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.[118] Similarly, the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) allows the disclosure of information where the information concerns matters outside Australia and the Director-General of the Australian Security Intelligence Organisation (ASIO) 'is satisfied that the national interest requires the communication'.[119]

7.111 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'.[120]

7.112 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.[121]

Public interest disclosure legislation

7.113 As discussed in Chapter 2, public interest disclosure, or 'whistleblowing', is 'the disclosure by organisation members (former or current) of illegal, immoral or

---

115 Ibid, Rec 21.
116 *Crimes Act 1914* (Cth) s 79(2)(a)(ii), (3)(b).
117 This exception is discussed further in Ch 3.
118 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 209.
119 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(b).
120 *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).
121 Australian Parliament—Senate Select Committee on Public Interest Whistleblowing, *In the Public Interest* (1994), [9.53].

illegitimate practices under the control of their employers to people or organisations that might be able to effect action'.[122] Public interest disclosures by Commonwealth officers may involve the unauthorised disclosure of information obtained because of a person's position as a Commonwealth officer, and therefore may attract administrative penalties or criminal sanctions under various secrecy provisions.

7.114 While there is currently limited protection at the Commonwealth level for people who make public interest disclosures, the Australian Government has indicated that it intends to develop public interest disclosure legislation in 2009.[123] As noted above, for the purposes of this Report the ALRC is proceeding on the basis that such legislation will be put in place, and that it will largely reflect the recommendations made in the *Whistleblower Protection* report.

7.115 A person who made a disclosure under the framework established by the proposed legislation would be protected from adverse action in the workplace and from criminal liability (including under the general secrecy offence), civil liability and administrative penalties.[124] In DP 74, the ALRC expressed the view that comprehensive public interest disclosure legislation was preferable to including a public interest disclosure exception in secrecy provisions. This was on the basis that public interest disclosure legislation has the potential to protect whistleblowers from criminal, civil and administrative sanctions and not just from prosecution under a particular provision. In DP 74, the ALRC proposed that the general secrecy offence should include a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation.[125]

Submissions and consultations

7.116 There was general support expressed in submissions for the introduction of public interest disclosure legislation[126] although CLA stated that the proposed model in the *Whistleblower Protection* report was too narrow.[127] CLA expressed support for the ALRC's proposal to include a cross reference in the general secrecy offence to the immunity provided by the proposed public interest disclosure legislation.[128]

---

122 A Brown, *Public Interest Disclosure Legislation in Australia* (2006), xxi.

123 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <www.smos.gov.au/speeches> at 6 December 2009.

124 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.

125 Recommendation 9–2.

126 Whistleblowers Australia, *Submission SR 74,* 17 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009; 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.

127 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

128 Ibid.

7.117 A number of stakeholders suggested, however, that in the absence of robust public interest disclosure legislation there should be an exception in the general secrecy offence for disclosures in the public interest.[129] The Australia's Right to Know coalition considered that the general secrecy offence and the subsequent disclosure offence should include an exception where the Commonwealth officer—and any third party recipient of the Commonwealth information disclosed—was acting honestly and reasonably to protect the public interest.[130]

7.118 Whistleblowers Australia, however, strongly endorsed the ALRC's view that robust public interest disclosure legislation was preferable to including public interest disclosure exceptions in secrecy provisions. This was on the basis that public interest disclosure legislation has the potential to protect whistleblowers from criminal, civil and administrative sanctions.[131]

7.119 Ron Fraser noted that individuals who were not covered by the proposed public interest disclosure legislation, but wished to make a public interest disclosure, might be caught by the subsequent disclosure offence. He suggested that such individuals should be protected from prosecution under the subsequent disclosure offence in the same circumstances that Commonwealth officers were protected from prosecution under the general offence. He noted that the *Whistleblower Protection* report had recommended that the government consider extending the protection provided by the proposed public interest disclosure legislation to cover members of the public who make disclosures about the public sector.[132]

ALRC's views

Public interest exception

7.120 The ALRC recommends, above, that a disclosure in accordance with an authorisation given by an agency head or minister that the disclosure would, on balance, be in the public interest should form an exception to the general secrecy offence.[133] This exception does not, however, provide scope for individual Commonwealth officers to disclose information on the basis of their own assessment that disclosure is in the public interest. This is appropriate, in the ALRC's view, because the general secrecy offence only criminalises the disclosure of information that does, or is reasonably likely to, or is intended to have very serious consequences such as damaging national security, defence or international relations or putting someone's life in danger. In these circumstances, the decision to disclose, despite the potentially serious consequences, should be taken at a senior level.

---

129 R Fraser, *Submission SR 78,* 21 August 2009; Community and Public Sector Union, *Submission SR 57,* 7 August 2009; L McNamara, *Submission SR 51,* 6 August 2009; AJ Brown, *Submission SR 44,* 18 May 2009; Australian Press Council, *Submission SR 16,* 18 February 2009.

130 Australia's Right to Know, *Submission SR 72,* 17 August 2009.

131 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.

132 R Fraser, *Submission SR 78,* 21 August 2009.

133 Recommendation 7–1(b).

7.121 However, in the ALRC's view, individual officers should have an avenue to express concerns about illegal, immoral or illegitimate practices under the control of their employers through public interest disclosure legislation.

Public interest disclosure legislation

7.122 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,[134] the ALRC has not had the opportunity to consider the final form of the legislation. For the purposes of this Report, the ALRC is proceeding on the basis that such legislation will be put in place and that it will largely reflect the recommendations made in the *Whistleblower Protection* report.

7.123 In the ALRC's view, a comprehensive and robust public interest disclosure regime is preferable to including an express exception in the general secrecy offence for disclosures made in the public interest. The whistleblower protections recommended by the Standing Committee include immunity from criminal liability and so will provide protection from prosecution under the general secrecy offence for disclosures made within the public interest disclosure framework. Again, because the general secrecy offence only criminalises the disclosure of information that is likely to have serious consequences, it is important that any such disclosure should take place within the framework and safeguards provided by the proposed public interest disclosure regime, rather than simply on the basis of an assessment made by an individual Commonwealth officer.

7.124 The ALRC is not recommending 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. It is unnecessary from a legal perspective, and it would be inconsistent to include a note of this nature in the general offence and not to include a similar note in all other secrecy provisions. Instead, the interaction between secrecy laws and public interest disclosure legislation should be set out in information-handling policies and guidelines[135] and included in employee training and development initiatives.[136]

7.125 As explained further below, in developing the public interest disclosure legislation, it will be important to ensure consistency with the general secrecy offence. In particular, the public interest disclosure legislation should cover at least the same categories of persons as those 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 subsequent disclosure offences recommended by the ALRC.

---

134 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <www.smos.gov.au/speeches> at 6 December 2009.

135 See discussion in Ch 14.

136 See discussion in Ch 15.

Categories of persons covered

7.126 The ALRC recommends that the new general secrecy offence cover a range of 'Commonwealth officers'.[137] Of these, 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.[138] In general terms, however, the ALRC's view is that to provide effective protection for whistleblowers, the public interest disclosure legislation should cover the same categories of people subject to the general secrecy offence. The statutory language used in the public interest disclosure legislation and the new general secrecy offence ultimately should be consistent in this regard.

Public interest disclosures to third parties

7.127 As discussed in Chapter 2, the public interest disclosure regime proposed by the Standing Committee would protect a person making a disclosure outside the formal internal and external channels—for example, to the media—in certain very limited circumstances. The Committee recommended that disclosure to a third party external to the public service would only be protected where the matter had already been disclosed internally, or to an external authority, but had not been acted on in a reasonable time and the matter threatened immediate serious harm to public health or safety.[139]

7.128 In developing public interest disclosure legislation, it will be important to ensure that a journalist or other person who further discloses information received by way of a protected public interest disclosure will not commit an offence—for example, under offences which cover the disclosure of information by 'any person'[140] or under the subsequent disclosure offences recommended in this Report.[141] 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 should also be immune from liability.

Subsequent disclosure of information received in confidence

7.129 One of the subsequent disclosure offences recommended by the ALRC would impose criminal sanctions on a third party for the unauthorised disclosure of

---

137 Recommendation 6–1.
138 Parliamentary privilege is discussed in Ch 16.
139 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Whistleblower Protection: A Comprehensive Scheme for the Commonwealth Public Sector* (2009), Rec 21.
140 For example, *Crimes Act 1914* (Cth) s 79.
141 Recommendations 6–6, 6–7.

information received from a Commonwealth officer on terms requiring it to be held in confidence.[142] This offence is intended to cover, for example, state and territory officers or private sector individuals who share sensitive Commonwealth information. It is possible that such third parties may be in a position to make public interest disclosures and in the ALRC's view this should be encouraged and the disclosures protected.

7.130 Public interest disclosure legislation could protect these individuals by way of a deeming provision. 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 disclosure.[143] The Standing Committee used the example of a former volunteer at 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'.[144] 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.

Recommendation 7–3 In developing public interest disclosure legislation the Australian Government should ensure that the legislation protects:

(a) individuals subject to the general secrecy offence;

(b) individuals who subsequently disclose Commonwealth information received by way of a protected public interest disclosure; and

(c) individuals subject to the subsequent disclosure offence for the unauthorised disclosure of information received from a Commonwealth officer on terms requiring it to be held in confidence.

Penalties

7.131 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

142 Recommendation 6–7.

143 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.

144 Ibid, [3.85].

offences to 'ensure [the] penalty fits with other penalties in Commonwealth law'.[145] 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.[146] This can only be achieved if the maximum penalties specified for similar offences are also consistent. In the following section of the chapter, the ALRC, in keeping with this approach, recommends a penalty regime for the general secrecy offence and the subsequent disclosure offences.

Penalties in existing secrecy provisions

7.132 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, the court may impose instead of, or in addition to, a penalty of imprisonment, a pecuniary penalty not exceeding 120 penalty units.[147]

7.133 Section 4B(3) of the *Crimes Act* 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.

7.134 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) of the *Crimes Act* 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;

- s 142.2 of the *Criminal Code* includes an offence for using official information where a Commonwealth public official intends 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;

---

145 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 38.

146 Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders*, ALRC 103 (2006), Rec 5–1(d).

147 At the time of writing, this amounts to $13,200: *Crimes Act 1914* (Cth) s 4AA.

- s 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 attracts a maximum penalty of 10 years imprisonment; and

- the espionage offences in the *Criminal Code*—which include communicating information concerning the Commonwealth's security or defence to another country intending to prejudice the Commonwealth's security or defence—these offences attract a maximum penalty of 25 years.

7.135 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.

Penalties for the general secrecy offence

7.136 In DP 74 the ALRC proposed a three-tier general secrecy offence with escalating penalties.[148] In relation to the first-tier offence—which attached strict liability to the requirement to prove harm—the ALRC proposed a maximum penalty of two years imprisonment, or a pecuniary penalty not exceeding 120 penalty units, or both. In relation to the second-tier offence—which required the prosecution to prove that the defendant knew, or was reckless as to whether, or intended the disclosure to harm personal privacy or commercial affairs—the ALRC proposed a maximum penalty of five years imprisonment, or a pecuniary penalty not exceeding 300 penalty units, or both. In relation to the third-tier offence—which required the prosecution to prove that the defendant knew, or was reckless as to whether, or intended the disclosure to harm the essential public interests discussed in Chapter 5—the ALRC proposed a maximum penalty of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.[149]

7.137 In light of other recommendations in this Report, it is no longer necessary to consider penalties for a three-tier general secrecy offence. In Chapter 6, the ALRC considers and rejects the proposal to include an offence that attaches strict liability to the requirement that the disclosure caused harm. In Chapter 5, the ALRC considers and rejects the proposal that the general secrecy offence cover disclosures that have a substantial adverse effect on personal privacy or commercial affairs. Because of this it

148 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–3.

149 Ibid, Proposal 9–3(b).

is only necessary to consider what penalty should attach to the single-tier general secrecy offence recommended in this Report.

Submissions and consultations

7.138 In its submission to IP 34, the AGD noted that currently most secrecy offences carry a maximum penalty of two years but that, where particularly sensitive or national security information was involved, the imposition of higher maximum penalties may be justified:

> 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.[150]

7.139 The Australian Commission for Law Enforcement Integrity (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, 240 penalty units, or both. The second tier addresses the unauthorised disclosure of official 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, 600 penalty units, or both. 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.[151]

ALRC's views

7.140 In Chapter 6, the ALRC recommends that the general secrecy offence should apply where a Commonwealth officer discloses Commonwealth information and knows, is reckless as to whether, or intends the disclosure will:

- damage the security, defence or international relations of the Commonwealth;
- prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences;

---

150 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
151 Australian Commission for Law Enforcement Integrity, *Submission SR 18,* 18 February 2009.

- endanger the life or physical safety of any person; or
- prejudice the protection of public safety.[152]

7.141 The disclosures covered by this offence involve potential harm of a high order, including endangering 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'.[153]

7.142 It is also consistent with the penalties imposed under s 79(2) of the *Crimes Act* and falls within the range of maximum penalties included in offence provisions with a harm requirement, discussed above. The ALRC recommends, therefore, in relation to the general secrecy offence a maximum penalty of seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both.

Recommendation 7–4 The general secrecy offence should stipulate a maximum penalty of seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both.

Penalties for the subsequent disclosure offences

7.143 In Chapter 6, the ALRC proposes the creation of two offences for the subsequent disclosure of Commonwealth information in certain circumstances. The offences would be committed where a third party subsequently disclosed information without authority and a Commonwealth officer had initially disclosed the information:

- in breach of the general secrecy offence;[154] or
- on terms requiring it to be held in confidence.[155]

7.144 In relation to both offences, it would be necessary to show that the person who received the information and then subsequently disclosed it without authority knew, or was reckless as to whether, the subsequent disclosure of the information would harm, or was reasonably likely to harm, one of the public interests set out in Recommendation 5–1.

---

152 Recommendation 6–5.
153 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 35.
154 Recommendation 6–6.
155 Recommendation 6–7.

7.145 In DP 74, the ALRC proposed only one subsequent disclosure offence, but that the offence should have two tiers, the first tier dealing with disclosures that harmed personal privacy or commercial affairs and the second tier dealing with disclosures that harmed public interests similar to those set out in Recommendation 5–1. The ALRC also proposed that the maximum penalties for the equivalent tiers in the general secrecy offence and the subsequent disclosure offence should be consistent.[156]

7.146 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)[157] and the *Aged Care Act*.[158]

7.147 The *Guide to Framing Commonwealth Offences* sets out penalty benchmarks for certain classes of offences.[159] 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[160] and subsequent[161] unauthorised handling of Commonwealth information.

Submissions and consultations

7.148 In its submission to IP 34, 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.[162]

7.149 A number of other stakeholders agreed that the same penalty should apply to both initial and subsequent disclosures,[163] with ASIC noting that the potential harm arising from both the initial and subsequent disclosures is the same.[164]

---

156 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposals 9–4, 9–5.

157 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 121(2), 127.

158 *Aged Care Act 1997* (Cth) ss 86-2, 86-5.

159 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 47.

160 *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).

161 *Australian Hearing Services Act 1991* (Cth) s 67(8).

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

163 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 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.

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

7.150 On the other hand, the Public Interest Advocacy Centre's (PIAC) view was that the penalties for subsequent disclosure should be lower, 'except where intent to damage Australia's national interest is proven'.[165]

ALRC's views

7.151 In the ALRC's view, the level of culpability and potential harm encompassed by the subsequent disclosure offences is of a similar order to that reflected in the recommended general secrecy offence. The ALRC recommends, therefore, that the maximum penalties stipulated in the subsequent disclosure offences should be the same as the maximum penalty stipulated in the general secrecy offence.

Recommendation 7–5 The subsequent disclosure offences should stipulate maximum penalties of seven years imprisonment, a pecuniary penalty not exceeding 420 penalty units, or both.

Other issues

Consent of the Attorney-General to prosecute

7.152 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 of the *Crimes Act*[166] or s 91.1 of the *Criminal Code* dealing with espionage.[167] 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 pt 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.[168]

7.153 Other secrecy provisions that require the consent of the Attorney-General to institute a prosecution include:

- ss 18 and 92 of the ASIO 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

---

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

166 *Crimes Act 1914* (Cth) s 85. The Attorney-General's consent is not required for prosecutions under s 70 of the *Crimes Act.*

167 *Criminal Code* (Cth) s 93.1.

168 Revised Explanatory Memorandum, Criminal Code Amendment (Espionage and Related Matters) Bill 2002 (Cth).

- various provisions of the *Intelligence Services Act 2001* (Cth), including the communication of information prepared by or on behalf of the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation or the Defence Signals Directorate by officers of the respective agency,[169] and publication by any person of the identity of the staff of these agencies.[170]

7.154 Other types of offences that require the Attorney-General's consent in order to commence prosecutions include:

- sedition;[171]
- those involving harming Australians outside of Australian territory;[172] and
- genocide, crimes against humanity, war crimes and crimes against the administration of justice in the International Criminal Court.[173]

7.155 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.[174] The CDPP *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'.[175]

7.156 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.[176]

---

169 *Intelligence Services Act 2001* (Cth) ss 39, 39A and 40, respectively.

170 Ibid s 41. See also *Intelligence Services Act 2001* (Cth) sch 1 pt 2 cl 13, which requires the consent of the Attorney-General to prosecute members of the Parliamentary Joint Committee on Intelligence and Security for offences under that Act.

171 *Criminal Code* (Cth) s 80.5.

172 Ibid s 115.6.

173 Ibid s 268.121.

174 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* (2009), [2.24].

175 Ibid, [2.26].

176 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 1983* (Cth), the CDPP can take over a private prosecution and terminate it.

7.157 In its Inquiry into federal sedition laws, the ALRC raised concerns about the political nature of consent requirements.[177] Specifically, the Attorney-General, as a political figure, might be perceived to agree more readily to the prosecution of certain individuals—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.[178] The Australian Government expressed support for this recommendation.[179]

7.158 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.

7.159 In DP 74, the ALRC expressed the view that the general secrecy offence should not include a requirement to seek the Attorney-General's consent prior to commencing a prosecution. The ALRC suggested that any directions from the Attorney-General to the CDPP in relation to such prosecutions might be included in directions or guidelines issued under s 8 of the *Director of Public Prosecutions Act* as it would ensure a level of transparency around any intervention in the prosecutorial decision making process by the Attorney-General.

Submissions and consultations

7.160 In its submission, the CDPP noted that the power under s 8 of the *Director of Public Prosecutions Act* has rarely been exercised and that it is a formal process requiring tabling in Parliament and gazettal. The CDPP expressed the view that this power would not be an appropriate alternative to a consent requirement in relation to individual prosecutions.[180]

7.161 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

177 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Ch 13.

178 Ibid, Rec 13–1.

179 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.

180 Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009.

> 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.[181]

7.162 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.[182]

7.163 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.[183]

7.164 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.[184]

7.165 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.[185]

ALRC's views

7.166 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.[186] Given the reasons outlined in that report, the ALRC does not recommend that the new

---

181 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
182 Australian Intelligence Community, *Submission SR 37,* 6 March 2009.
183 Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.
184 The Treasury, *Submission SR 22,* 19 February 2009.
185 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009.
186 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Rec 13–1.

general secrecy offence should include a requirement for the consent of the Attorney-General prior to the commencement of a prosecution under the provision.

7.167 In addition, and on the basis of the CDPP's advice, discussed above, the ALRC does not recommend that the Attorney-General should provide directions or guidelines in relation to particular prosecutions under the general secrecy offence under s 8 of the *Director of Public Prosecutions Act*. The formal process required in relation to such directions or guidelines is unlikely to be consistent with timeliness requirements in relation to individual cases. In the ALRC's view, the decision to prosecute should remain with prosecuting authorities.

Injunctions

7.168 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.

7.169 In its report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC analysed potential mechanisms to prevent the disclosure of classified and security sensitive Commonwealth information in these circumstances.[187] The ALRC considered that injunctions to restrain a breach of the criminal law provided an appropriate vehicle. However, in the absence of an express statutory power, courts have traditionally been reticent to issue such injunctions.[188]

7.170 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'.[189] 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.[190]

7.171 In the ALRC report, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, it was noted that injunctions are not in themselves penalties but

---

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

188 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.

189 Ibid, 481.

190 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50. Mason J held that s 79 of the *Crimes Act* was not such a provision.

may be used in support of actions seeking penalties.[191] 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.[192]

7.172 Section 17B of the *Taxation Administration Act* is an example of a provision that expressly provides for injunctive relief in relation to the disclosure of information:

> 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.[193]

7.173 The Tax Laws Exposure Draft Bill also proposes 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.[194] 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 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).[195]

7.174 In *Keeping Secrets*, the ALRC noted the 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.[196]

---

191 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [2.115].

192 Australian Securities & Investments Commission, *Consultation,* Sydney, 23 May 2001.

193 *Taxation Administration Act 1953* (Cth) s 17B(1).

194 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 item 1 cl 355-330.

195 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [7.8].

196 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–1.

7.175 In DP 74, the ALRC proposed 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.[197]

Submissions and consultations

7.176 Stakeholders were generally supportive of providing the courts with power to issue injunctions to restrain the unauthorised disclosure of Commonwealth information.[198] 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.[199]

7.177 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.[200] 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).[201]

7.178 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.[202]

7.179 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

---

197 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–6.

198 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Australian Intelligence Community, *Submission SR 77,* 20 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009.

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

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

201 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

202 The Treasury, *Submission SR 22,* 19 February 2009.

> 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.[203]

7.180 The Australian Privacy Foundation was of the view that the power to issue an injunction should extend to prevent any subsequent disclosure of Commonwealth information initially disclosed without authority.[204]

ALRC's views

7.181 There was significant support among stakeholders for the inclusion of an express power to issue injunctions in secrecy offences.

7.182 The 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 5. In the ALRC's view, these public 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, a court will be required to consider the potential for the disclosure to cause harm to the listed public interests.

7.183 The ALRC recommends that the general secrecy offence, and the subsequent disclosure offences, 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 disclosure of the information.

Recommendation 7–6 The general secrecy offence and the subsequent disclosure offences 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 disclosure of the information.

---

203 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.
204 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

8. The Role of Specific Secrecy Offences

Contents

Introduction

8.1 In this Report, the ALRC recommends the creation of a new general secrecy offence that would make it an offence for a current or former Commonwealth officer to disclose information that causes, or was likely or intended to cause, harm to specified public interests.[1]

8.2 The ALRC does not, however, consider that the new general secrecy offence should be the only criminal provision regulating the unauthorised disclosure of Commonwealth information. There is still a need for specific secrecy offences tailored to the needs of particular agencies; or to the protection of certain kinds of information; or to cover people other than Commonwealth officers. Chapters 8 to 11 consider the circumstances in which separate secrecy offences are warranted, and what such offences should look like.

When are secrecy offences warranted?

8.3 A central aim of this Inquiry is to develop a principled approach to the imposition of criminal penalties for the unauthorised disclosure of Commonwealth information. Chapter 4 sets out the ALRC's recommended framework for the regulation of individuals who handle government information. At its core, the

1 Recommendation 5–1.

framework reserves criminal penalties only for conduct that may cause harm to essential public interests.

8.4 In Chapter 5, the ALRC considers which public interests should be protected in the general secrecy offence, and recommends that the following categories be included:

- national security, defence and international relations of the Commonwealth;
- prevention, detection, investigation, prosecution or punishment of criminal offences;
- life or physical safety of any person; and
- protection of public safety.[2]

8.5 For the reasons discussed in Chapter 5, the ALRC considers that to warrant a criminal penalty, disclosures must harm more than the effective working of government or commercial or personal interests.

8.6 The same policy rationale should inform the consideration of specific secrecy offences. In order to be consistent with Australia's international obligations, for a criminal offence to be committed, there should be a reasonable likelihood that the disclosure of the information will harm an essential public interest. Where no such harm is likely, the ALRC considers that other responses to the unauthorised disclosure of Commonwealth information are appropriate—including the imposition of administrative sanctions or the pursuit of contractual or general law remedies.

8.7 This chapter discusses how specific secrecy offences can be framed in order to ensure that they are targeted only to harmful conduct that warrants criminal sanction. The discussion compares two ways of confining secrecy provisions to appropriate harms: first, including an express requirement of harm in specific secrecy offences; and secondly, protecting certain categories of information in which the harm of disclosure may be implicit or not amenable to inclusion as an element in a criminal offence.

Express requirement of harm

8.8 There are precedents for the inclusion of an express harm requirement in secrecy offences. A small number of secrecy offences currently include a requirement that the disclosure cause, or be likely to cause, a particular harm. As the following examples illustrate, a harm requirement may either take the form of an objective test or refer to the intention of the person making a disclosure:

---

2 Recommendation 5–1.

- s 58 of the *Defence Force Discipline Act 1982* (Cth), which requires that a disclosure 'is likely to be prejudicial to the security or defence of Australia' in order for an offence to be committed;

- s 71(5) of the *Pooled Development Funds Act 1992* (Cth), which 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';

- s 758 of the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* (Cth), which prohibits the disclosure of information where it 'could reasonably be expected to prejudice substantially the commercial interests of another person';

- sch 3, item 6 of the *Wheat Export Marketing (Repeal and Consequential Amendments) Act 2008* (Cth), which requires that a disclosure 'could reasonably be expected to cause financial loss, directly benefit a consumer or reduce the return of the pool';[3] and

- s 79(2) of the *Crimes Act 1914* (Cth), which prohibits the communication of certain information 'with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions'.

8.9 A few other secrecy offences define the protected information by reference, in part, to identifiable harms. 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'.[4] '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.[5]

8.10 In most cases, however, harm is not an express element of the offence, and therefore, the prosecution is not required to prove harm beyond reasonable doubt.

8.11 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC proposed 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

---

3 This provision continues the operation of s 5E of the now repealed *Wheat Marketing Act 1989* (Cth).

4 *Food Standards Australia New Zealand Act 1991* (Cth) s 114(1).

5 Ibid s 4(1). However, the meaning of 'confidential commercial information' is not always defined: see, eg, the *National Health and Medical Research Council Act 1992* (Cth) s 80.

information will cause harm to some specified public interest, except where there are countervailing public interests.[6]

8.12 There are several reasons in favour of including an express requirement of harm in specific secrecy offences. First, as discussed above and in Chapter 4, the fact that a disclosure causes, or was likely or intended to cause, harm is a principled basis for imposing a criminal penalty—without such harm, criminal penalties are unlikely to be justified.

8.13 Secondly, an express requirement of harm would narrow the scope of overly broad secrecy provisions. For example, in response to the Issues Paper, *Review of Secrecy Laws* (IP 34),[7] the Law Council of Australia considered that a harm requirement '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'.[8] The inclusion of a harm requirement would mean that criminal penalties would not apply to *all* disclosures of *any* information, but only to disclosures that have the potential to harm public interests.

Submissions

8.14 The response of stakeholders to the proposal that specific secrecy offences should generally incorporate a requirement that the disclosure of information cause, or is likely or intended to cause, harm to a specified public interest was mixed. The issues were captured in the submission from the Australian Government Attorney-General's Department (AGD), which acknowledged 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'.[9] However, the AGD suggested 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' and concluded that a 'reasonably likely to cause harm' formulation would be a useful model for some secrecy offences.[10]

8.15 A number of stakeholders agreed with the ALRC's proposal that specific secrecy provisions should generally incorporate a requirement of harm, except in exceptional cases.[11] The Community and Public Sector Union (CPSU) submitted, however, that specific secrecy offences should always incorporate a reasonable

---

6 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 10–1.
7 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).
8 Law Council of Australia, *Submission SR 30,* 27 February 2009.
9 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
10 Ibid.
11 Community and Public Sector Union, *Submission SR 57,* 7 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

likelihood of harm criteria.[12] Ron Fraser agreed, suggesting that the proposed exception for circumstances where there are clear countervailing public interests was unnecessary.[13]

8.16 Most government stakeholders opposed the inclusion of an express harm requirement in a number of specific secrecy offences. A number considered that an express harm requirement was unnecessary, because the harm to public interests was implicit in specific offences dealing with the unauthorised disclosure of sensitive information.[14] For example, the Department of Health and Ageing submitted that, because of the 'sensitivity of health information',

> maintaining continuous public trust and confidence in the protection of health information held by the department is a key concern. That the release of secret information would be reasonably likely to harm the public interest is already implicit in the existing health secrecy provisions.[15]

8.17 The Treasury argued that consideration of public interest—and harm to those interests—properly occurs when a secrecy provision is drafted. Referring to submissions quoted in IP 34, and the concerns that secrecy provisions are 'too broad and contrary to the interests of Government transparency', the Treasury suggested that:

> Rather than what would, in effect, be a two-stage consideration of how sensitive particular material might be, these concerns might be more effectively addressed through ensuring that the initial judgment of when material is 'secret' is appropriately limited (by ensuring, for instance, as is the case with secrecy provisions relating to agencies such as [the Australian Prudential Regulation Authority] and the [Australian Taxation Office], that these provisions are designed to give effect to the public expectation that the confidentiality of information provided to Government is respected.[16]

8.18 Some agencies considered that the very nature of certain kinds of information means that disclosure will inevitably cause harm. For example, the AGD submitted that it is not necessary to include an express harm requirement where secrecy provisions protect certain categories of information, such as national security, intelligence and defence information, law enforcement information and Cabinet documents.[17]

---

12 Community and Public Sector Union, *Submission SR 57,* 7 August 2009.

13 R Fraser, *Submission SR 78,* 21 August 2009.

14 Australian Federal Police, *Submission SR 70,* 14 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009; Australian Prudential Regulation Authority, *Submission SR 52,* 6 August 2009; Department of Human Services, *Submission SR 26,* 20 February 2009.

15 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.

16 The Treasury, *Submission SR 60,* 10 August 2009.

17 Attorney-General's Department, *Submission SR 67,* 14 August 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009.

8.19 The Australian Transaction Reports and Analysis Centre (AUSTRAC) submitted that the disclosure of the information it holds—comprising financial transaction data and compliance information from 17,000 reporting entities and foreign government financial intelligence units—is, by its nature, likely to cause harm to national security, law enforcement, personal privacy or commercial affairs, and 'therefore the incorporation of a harm element is of little value'.[18]

8.20 Other agencies were of the view that *any* unauthorised disclosure of personal information held by their agency would always harm the public interest. For example, the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) considered that:

> any unauthorised disclosure, regardless of whether there is any intention of harm against a specified public interest in a particular instance, would inherently harm the public interest. This is because any unauthorised disclosure could have the potential to erode public confidence in the protection of information held in departmental records.[19]

8.21 The Australian Taxation Office (ATO) noted that the harm caused by the unauthorised disclosure of taxpayers' personal information not only impacts upon a person's privacy, but also the integrity of the taxation system and individuals' compliance with it. The ATO argued that this kind of harm would be difficult to capture in the wording of a criminal offence provision:

> The ATO acknowledges that broadly it could be argued that public harm, in terms of a lessening of confidence in the privacy and confidentiality of information held by it could result from disclosures of taxpayer information. However, this would be practically difficult to apply because surely a certain number of disclosures of information would need to occur before this ambit type of harm could possibly be made out in a criminal prosecution.[20]

8.22 In response to submissions from government agencies that the harm justifying some secrecy provisions is implicit, Ron Fraser submitted that 'in most existing secrecy provisions, the harm that is involved, even though currently implied, should not be difficult to specify'.[21]

8.23 Fraser also stressed that there were sufficient other means to ensure public confidence in the protection of personal information:

> The general offence, the provisions of the *Privacy Act* [*1988* (Cth)], non-criminal legislative provisions protecting specific information where thought necessary ... and administrative penalties, will provide the reassurance that the public requires that

---

18 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

19 Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009. FaHCSIA also raised concerns that a harm test would create uncertainty for officers, and cause difficulties in proving harm when prosecuting offences. These issues are dealt with in detail in Ch 5 in relation to the general secrecy offence, and are not revisited in this chapter.

20 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

21 R Fraser, *Submission SR 78,* 21 August 2009.

sensitive information they provide to agencies, or which agencies collect, will be protected from unauthorised disclosure.[22]

ALRC's views

8.24 An express requirement that an unauthorised disclosure cause, or be likely or intended to cause, harm will be appropriate where a secrecy offence covers a wide range of information, not all of which is necessarily likely to cause harm to a public interest if disclosed. This would confine the scope of the offence to those disclosures that actually involve the risk of harm to public interests.

8.25 Unlike the general secrecy offence, specific secrecy offences can be targeted to particular kinds of information and regulate the conduct of particular parties. Therefore, in very limited circumstances, the way in which secrecy offences are framed, and the context in which they operate, provide a sufficient likelihood that harm will be caused by an unauthorised disclosure, making an express requirement of harm unnecessary in every case.

8.26 Further, the harm caused by the disclosure of some kinds of information may not be amenable to inclusion as an element of an offence to be proved beyond reasonable doubt.

8.27 The following section discusses some circumstances where it may not be necessary to include an express requirement of harm in specific secrecy offences due to the nature of the information protected or the context in which a provision operates.

Protecting categories of information

8.28 Many secrecy offences currently prohibit the unauthorised handling of specific categories of Commonwealth information. These include, for example, offences that relate to the disclosure of:

- personal information,[23] or information concerning or relating to the affairs of another person;[24]

22 Ibid.

23 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).

24 See, eg, *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).

- confidential commercial information[25] or other information that is supplied in confidence;[26]

- defence or national security information, or information the unauthorised disclosure of which may prejudice defence or national security;[27]

- law enforcement and intelligence information—information about the operations or investigations of law enforcement agencies;[28]

- taxation information—information provided by a taxpayer to a person or an agency pursuant to a legislative requirement contained in taxation legislation;[29]

- census and statistical information—information collected and maintained by the ABS under the *Census and Statistics Act 1905* (Cth);[30] and

- electoral information—information collected and maintained by the Australian Electoral Commission under the *Commonwealth Electoral Act 1918* (Cth).[31]

8.29 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'.[32] The challenge is to determine what kinds of information are so sensitive that *any* unauthorised disclosure of information from within that category is sufficiently harmful to an essential public interest to justify the application of criminal sanction, without the express stipulation that the disclosure cause harm.

8.30 In DP 74, the ALRC asked in what circumstances is it inappropriate for a secrecy offence to require that a disclosure be reasonably likely to cause harm. The ALRC provided national security classified information, or information concerning the defence or international relations of the Commonwealth, as examples of possible categories of information that may justify this approach.

---

25 See, eg, *Gene Technology Act 2000* (Cth) s 187; *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s 162(1).

26 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.

27 See, eg, *Criminal Code* (Cth) s 91.1; *Designs Act 2003* (Cth) s 108; *Defence Force Discipline Act 1982* (Cth) s 58; *Defence Act 1903* (Cth) s 73A.

28 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 92; *Australian Crime Commission Act 2002* (Cth) s 29B; *Australian Federal Police Act 1979* (Cth) s 40ZA.

29 See, eg, *Inspector-General of Taxation Act 2003* (Cth) s 37(2); *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 55; *Child Support (Assessment) Act 1989* (Cth) s 150(2).

30 *Census and Statistics Act 1905* (Cth) ss 19, 19A.

31 *Commonwealth Electoral Act 1918* (Cth) ss 90B, 91B, 189B, 323.

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

8.31 Submissions identified three general circumstances in which it may be appropriate for a specific secrecy offence not to include an express requirement of harm: first, where the secrecy offence regulates intelligence agencies; secondly, where the secrecy offence regulates law enforcement agencies; and thirdly, where disclosure would harm confidence in, and compliance with, key government regulatory bodies.

8.32 These three areas—and possible further categories—are discussed in turn below using the framework set out in Chapter 4. In relation to each, the ALRC considers whether an express requirement of harm is sufficient to prevent the harm to the public interest that arises from the disclosure of certain information. If not, the ALRC then considers how specific secrecy offences can be framed to ensure that the offence is necessary and proportionate to the protection of essential public interests.

Information obtained or generated by intelligence agencies

8.33 National security and intelligence information are frequently cited as special kinds of information that require stringent protection from unauthorised disclosure because of the inherent sensitivity of the information and the high risks associated with disclosure or misuse.

Overview of secrecy offences that apply to intelligence agencies

8.34 Information obtained or generated by the Australian Intelligence Community (AIC) is currently protected by several specific secrecy provisions.[33] Section 18 of the *Australian Security Intelligence Organisation Act 1979* (Cth) makes it an offence for a person to communicate information which was:

- prepared by or on behalf of the Australian Security Intelligence Organisation (ASIO) in connection with its functions, or in relation to the performance by ASIO of its functions; and

- acquired by the person by reason of his or her being, or having been, an officer or employee of ASIO, or having entered into any contract, agreement or arrangement with ASIO.

8.35 The *Intelligence Services Act 2001* (Cth) contains similarly phrased offences for the disclosure of information by staff, contractors and others who handle information prepared by or connected with the Australian Secret Intelligence Service (ASIS), the Defence Imagery and Geospatial Organisation and the Defence Signals Directorate. Two agencies in the AIC, the Office of National Assessments and the Defence

33 The Australian Intelligence Community comprises the Office of National Assessments, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Defence Intelligence Organisation, the Defence Imagery and Geospatial Organisation and the Defence Signals Directorate.

Intelligence Organisation, have not been regulated by separate specific secrecy offences.

8.36 These offences have limited application to particular kinds of information—information acquired or prepared by, or on behalf of, the organisation in connection with its functions, or information that relates to the performance of its functions—and to particular persons who, either through employment or agreement or arrangement, handle that information. These provisions do not expressly require that a disclosure cause, or was likely or intended to cause, any harm to the public interest. Rather, there is an implicit assumption that it is inherently harmful to disclose such information.

8.37 Section 1(1) of the *Official Secrets Act 1989* (UK) takes a different, but comparable, approach to the Australian provisions. Section 1(1) provides that:

> A person who is or has been—
>
> (a) a member of the security and intelligence services; or
>
> (b) a person notified that he is subject to the provisions of this subsection,
>
> is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

8.38 Section 1(1) makes it an offence for members of the security and intelligence agencies to disclose information relating to security or intelligence. Section 1(1) also covers people who have been notified in writing by a Minister of the Crown that they are subject to the provision. A notice may be served if, in the Minister's opinion, the work undertaken by a person is connected with the security and intelligence services and its nature is such that the interests of national security require that he or she should be subject to s 1(1).[34] As in the Australian secrecy offences applying to the AIC, s 1(1) of the *Official Secrets Act* does not include an express requirement that the disclosure cause harm.

8.39 However, where the *Official Secrets Act* regulates the disclosure of security or intelligence information by Crown servants and government contractors who are not members of the security and intelligence services, a disclosure of information relating to intelligence or security is an offence only if it is a 'damaging' disclosure.[35] That is, where a disclosure is made by a person outside the security and intelligence agencies, the prosecution has to show that the disclosure was likely to damage the operation of the security or intelligence service.[36]

---

34 *Official Secrets Act 1989* (UK) s 1(6).
35 Ibid s 1(3).
36 Ibid s 1(4).

8.40 The reason for making a distinction between members and former members of security and intelligence services and disclosures by other persons was explained in the White Paper preceding the 1989 reforms to the *Official Secrets Act*:

> While the government believes that this proposed test of harm is in general adequate to safeguard the interests both of the defendant and of the security and intelligence services, it considers that different arguments apply to the unauthorised disclosure of information by members or former members of those services. It takes the view that all such disclosures are harmful to the public interest and ought to be criminal. They are harmful because they carry a credibility which the disclosure of the same information by any other person does not, and because they reduce public confidence in the services' ability and willingness to carry out their essentially secret duties effectively and loyally. They ought to be criminal because those who become members of the services know that membership carries with it a special and inescapable duty of secrecy about their work. Unauthorised disclosures betray that duty and the trust placed in the members concerned, both by the State and by the people who give information to the services.[37]

8.41 The 1991 report *Review of Commonwealth Criminal Law* (the Gibbs Committee report), took a similar approach and considered that information obtained or generated by intelligence agencies ought to be protected by criminal sanctions:[38]

> 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 … [T]he Review Committee is satisfied that disclosures by such persons should be prohibited by criminal sanctions without proof of harm.[39]

8.42 Specific secrecy offences relating to intelligence and security agencies which do not include an express harm requirement place a higher duty on members of those agencies, in recognition of the sensitivity of the information they handle, and the higher duties of secrecy associated with their work.

Compatibility with international human rights obligations

8.43 Laws that restrict the right to freedom of expression set out in the ICCPR are permitted where they are necessary and proportionate for the protection of national security.[40] So, for example, the European Court of Human Rights has recognised that the 'proper functioning of a democratic society based on the rule of law may call for institutions like [intelligence services] which, in order to be effective, must operate in secret and be afforded necessary protection'.[41] The question is whether a law creating a

---

37 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [41].

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

39 Ibid, 323.

40 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 19(3).

41 *Vereniging Weekblad Bluf! v The Netherlands* (1995) 20 EHRR 189, [35].

criminal offence for the disclosure of any information obtained or generated by an intelligence agency is necessary and proportionate to the protection of national security.

8.44 There has been no consideration of the AIC secrecy provisions by the United Nations Human Rights Committee. However, the compatibility of s 1(1) of the *Official Secrets Act 1989* (UK) with art 10 of the *European Convention of Human Rights,*[42] which sets out the right to freedom of expression, was considered by the House of Lords in *R v Shayler.*[43] This case concerned a former member of the security services who had disclosed documents relating to security or intelligence matters to a national newspaper. While the House of Lords' decision relates to the *European Convention of Human Rights,* and is not therefore directly relevant to Australia, it gives some insight into issues that may inform the consideration of the AIC secrecy offences against human rights standards.

8.45 As noted in Chapter 2, the House of Lords noted that the provision was broadly framed, did not include a public interest defence and, unlike other provisions of the *Official Secrets Act,* did not require that the disclosure be 'damaging'.[44] However, it held that s 1(1) was compatible with the freedom of expression guaranteed by the *European Convention of Human Rights*.[45]

8.46 Critical to the House of Lords' decision was the fact that the prohibition on disclosure was not an 'absolute ban', in that there were 'sufficient and effective safeguards' to allow a person to communicate information. Lord Bingham of Cornhill discussed two lawful avenues available to communicate any concerns about the work of the security service. The first was a disclosure to a Crown servant for the purposes of his functions under s 7 of the Act, which would include disclosure to:

- a staff counsellor or an independent high-ranking civil servant appointed specifically to address concerns of the security and intelligence services;[46]
- relevant law enforcement authorities in the case of concerns about the lawfulness of the conduct; or
- several ministers, the secretariat to the Parliamentary Intelligence and Security Committee or to a number of integrity agencies in the case of concerns about misbehaviour or maladministration.[47]

---

42 Article 10 of the *European Convention of Human Rights* is in similar terms to art 19 of the *International Covenant on Civil and Political Rights.*

43 *R v Shayler* [2003] 1 AC 247.

44 Ibid, 276–277.

45 *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, ETS No. 5, 213 UNTS 221, (entered into force generally on 3 September 1953).

46 A non statutory office introduced in 1988: see House of Commons, *Parliamentary Debates*, 21 December 1988, col 467.

47 *R v Shayler* [2003] 1 AC 247, 270.

8.47 A second avenue for lawful disclosure was to seek official authorisation for the disclosure from a superior officer. Section 7 of the *Official Secrets Act* provides that a disclosure is made with lawful authority if it is made 'in accordance with an official authorisation'. Lord Hope of Craighead noted, however, that this provision could be criticised, particularly on the basis that it does not identify criteria that officials should consider when deciding whether or not to authorise a disclosure. Despite this, their Lordships considered that a decision to grant or deny authorisation could be subject to judicial review, on human rights as well as administrative grounds.[48] Thus, Lord Hope considered that an effective system of judicial review, compatible with the *Human Rights Act 1998,* could 'provide the guarantees that appear to be lacking in the statute'.[49]

8.48 The existence of these safeguards, the special position of members of the security and intelligence services and the highly sensitive material they handle, meant that, in their Lordships' view, the interference with their right to freedom of expression did not go beyond that required to protect the public interest in national security.[50]

8.49 Section 1(1) of the *Official Secrets Act* has also been considered by the United Nations Human Rights Committee. While the Committee did not state that the provision itself was incompatible with art 19 of the ICCPR, it expressed concern about the way in which the provision was enforced. It noted that disclosures of information may be penalised under the *Official Secrets Act 1989* even where they are not harmful to national security, and that powers under the Act have been 'exercised to frustrate former employees of the Crown from bringing into the public domain issues of genuine public concern'. The Committee observed that:

> The State party must ensure that its powers to protect information genuinely related to matters of national security are narrowly utilized and limited to instances where the release of such information would be harmful to national security.[51]

Current classification system

8.50 In relation to intelligence information in Australia, it may be argued that a harm-based approach is already incorporated in the national security classification system, which governs all national security information held by government. The *Australian Government Protective Security Manual* requires all national security information to be given one of four national security markings based on an assessment of the consequences of the unauthorised disclosure of the information—the higher the

48 Ibid, 271, 284.
49 Ibid, 284–288.
50 Ibid, 276, 283–288, 296–299.
51 United Nations Human Rights Committee, *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant: Concluding Observations of the Human Rights Committee-United Kingdom of Great Britain and Northern Ireland*, CCPR/GBR/CO/6, 30 July 2008, [24]. The Human Rights Committee made similar observations in 2001.

classification, the greater the risk of perceived damage arising from unauthorised disclosure.[52]

8.51 There are concerns, however, that documents are often over-classified, or not re-classified as their national security sensitivity reduces over time.[53] In recognition of this issue, the UK government, when developing the *Official Secrets Act,* was not prepared to rely on the security classification of information as a default indication of the harm likely to be caused by the disclosure of the information. The 1988 White Paper stated that:

> The fact that a document will be classified at a certain grade is not evidence of likely harm; it is only evidence of the view of the person who awarded the classification. Moreover, it is evidence only of the view taken at the time of classification; circumstances may have changed by the date of the disclosure.[54]

Submissions and consultations

8.52 Stakeholders provided differing views about whether information held by intelligence agencies, or national security information more generally, required the protection of secrecy offences without an express requirement of harm.

8.53 The AIC outlined several reasons why secrecy provisions protecting national security and intelligence information should not be subject to a test of likely, intended or actual harm. First, the AIC submitted that the nature of intelligence and national security information meant that the compromise of information held by AIC agencies could cause serious damage to Australia's national security.[55] Secondly, the AIC noted that even small amounts of information could, when taken together with other information, compromise national security regardless of its initial security classification. For example, great care is required to ensure that intelligence officers are not publicly identified:

> Even seemingly innocuous pieces of information, such as the amount of leave available to ASIS or ASIO staff or their salary, can yield significant counterintelligence dividends to a foreign intelligence service because such information may help to identify ASIS or ASIO officers. Protection of the identity of ASIS and ASIO officers is critical to human intelligence collection as those officers are either working in foreign countries beyond the protection of the Australian Government or their identification can lessen the ability of ASIO and ASIS to perform their national security functions.[56]

---

52 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual (PSM)* (2005). The *Protective Security Manual* is discussed in Ch 14.

53 See, eg, Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004); Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Audit Report 7 (1999).

54 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [75].

55 Australian Intelligence Community, *Submission SR 77,* 20 August 2009.

56 Ibid.

8.54 The AIC also 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'.[57]

8.55 Finally, the AIC submitted that the proposed harm element is inconsistent with legislative policy in other areas regulating national security information, including rules preventing the disclosure of intelligence and counter-intelligence information to a court or during government administrative and reporting processes. The AIC also submitted that a harm requirement would be inconsistent with the *Freedom of Information Act 1982* (Cth) which currently exempts AIC information from disclosure.[58]

8.56 The AIC recommended that the existing secrecy laws that govern intelligence agencies and protect the identity of ASIS and ASIO officers should be retained, and be consistent across all AIC agencies.

8.57 Further to the concerns expressed by the AIC, the AGD noted that the process of proving the harm caused by the disclosure of national security information during a prosecution may cause further harm:

> In proving beyond a reasonable doubt that a disclosure was reasonably likely to cause harm to national security additional information in the form of evidence will need to be disclosed to the Court. Given the nature of this information, there will be a significant risk that further harm could be caused by the release of information, including through court processes.[59]

8.58 On the other hand, a number of stakeholders submitted that even national security, intelligence and law enforcement information should be subject to a requirement that the information be likely to cause harm.[60] Australia's Right to Know coalition of media organisations argued that:

> exemptions should not be crafted to apply as of right or merely because information is generated or held by intelligence and security agencies—the information itself, rather than simply its source, would need to be assessed to establish if it legitimately fell

---

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

58 Australian Intelligence Community, *Submission SR 77,* 20 August 2009. However, two stakeholders commented that the secrecy and freedom of information regimes seek to achieve different outcomes and may not be comparable: R Fraser, *Submission SR 78,* 21 August 2009; L McNamara, *Submission SR 51,* 6 August 2009. Chapter 16 discusses the interaction between secrecy provisions and freedom of information legislation.

59 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

60 Community and Public Sector Union, *Submission SR 57,* 7 August 2009; R Fraser, *Submission SR 78,* 21 August 2009.

> within a proposed exemption necessary for the protection of essential public interests.[61]

8.59 Similarly, Dr Lawrence McNamara argued that the omission of a requirement of harm will:

> shield security agencies in a way that, taken with the [*National Security Information (Criminal and Civil Proceedings) Act 2004*] and its effects, will remove information from the public eye which is not likely to cause harm if disclosed. AIC agencies have management, training, and administrative options available to them to ensure secrecy; criminal sanctions should be available only when harm from disclosure is intended, actual, or reasonably likely.[62]

8.60 In relation to issues regarding the burden of proof, McNamara argued that where information is in fact of a sensitive nature the burden of proving that there is a reasonable likelihood of harm arising from its disclosure could be easily met:

> While an individual may not be in a position to judge the likelihood of harm that could result from disclosure of any piece of information ... this would itself be relevant to the recklessness component of a fault element. That is, 'the circumstances' would include the individual's knowledge of the difficulty in judging the likelihood of harm when deciding to risk disclosing information, and thus it would be more easily established that a risk would be unjustifiable. As such, there is not that great a barrier to proving fault. Where information is in fact of such a sensitive nature that there is a reasonable likelihood of harm then the burden of proof should be met without great difficulty. ...
>
> In the context of information held by security agencies, where employees are aware of the difficulty of making judgments about its significance, it would be a very difficult argument [for a defendant] to sustain in a case where there was in fact a reasonable likelihood of harm, and where the fault element is recklessness.[63]

ALRC's views

8.61 The ALRC acknowledges stakeholders' concerns about secrecy offences based on categories of information, particularly the concern that, while a category may be directed to protecting a legitimate public interest, the disclosure of information within that category will not always cause, or be likely to cause, harm. In addition, the ALRC notes the findings of previous reports that the security classification assigned to information is not necessarily an accurate indicator of the harm that could be caused by the unauthorised disclosure of the information. Therefore, the ALRC is not recommending the enactment of specific secrecy offences that cover 'national security classified information', preferring instead an approach that recognises that particular government agencies that obtain and generate sensitive information of this kind may need an agency-specific secrecy offence.

---

61 Australia's Right to Know, *Submission SR 72,* 17 August 2009.
62 L McNamara, *Submission SR 51,* 6 August 2009.
63 Ibid.

8.62 The ALRC considers that a prohibition on the disclosure of information obtained or generated by intelligence agencies is justified by the sensitive nature of the information and the special duties and responsibilities of officers and others who work in and with such agencies. The existing AIC secrecy offences cover a limited range of people who handle intelligence information, namely officers and employees, and people with whom the agency has an agreement or arrangement. The ALRC considers that it is appropriate for people in this position to be subject to higher responsibilities to protect inherently sensitive intelligence information.

8.63 The 'mosaic approach' argument put by the AIC—the argument that isolated disclosures of seemingly innocuous information, when combined with other information, together disclose sensitive information that could cause harm to national security—suggests that a secrecy offence that included an express requirement of harm would be insufficient to protect against harm to national security.

8.64 In coming to this view, the ALRC is not persuaded by the argument put by some agencies that a requirement that the prosecution prove harm, or likely harm, to national security in establishing an offence will necessarily cause further harm through the disclosure of sensitive information to the court. The *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) establishes procedures to protect information likely to prejudice national security from disclosure in federal criminal proceedings.[64]

8.65 However, while the ALRC accepts that specific secrecy offences covering the disclosure of information obtained or generated by or on behalf of the AIC by officers in AIC agencies, or people subject to an agreement or arrangement with the AIC, do not necessarily need an express requirement of harm, care must be taken to ensure that this approach is consistent with Australia's human rights obligations.

8.66 As discussed by the House of Lords in *R v Shayler*, it is important that secrecy offences do not constitute an absolute bar on the disclosure of information and, in order for the restriction on freedom of expression to be necessary and proportionate, some safeguards are required. *R v Shayler* considered two safeguards: first, avenues for authorised disclosures of concerns by officers in the intelligence services; and secondly, procedures for seeking authorisation for making particular disclosures.

8.67 In relation to the first safeguard, the Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer with responsibility for reviewing

---

64 The *National Security Information (Criminal and Civil Proceedings) Act 2004* (Cth) was enacted following a report by the ALRC on protecting national security information during court proceedings: Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004). However, the Act deals only with certain aspects of federal criminal proceedings and does not canvass the broader range of issues considered by the ALRC.

AIC agencies.[65] As part of this oversight role, the IGIS can receive reports and complaints concerning AIC activities and undertake formal inquiries. The IGIS may also undertake 'own motion' investigations into any matter that relates to an agency's compliance with the law, the propriety of the agency's actions and procedures, and any act or practice that may be inconsistent with human rights and discrimination law. However, the ability of the IGIS to inquire into particular matters varies according to which AIC agency is involved.[66]

8.68 An additional avenue for the disclosure of concerns by AIC officers could be created through proposed whistleblower protection laws. The House of Representatives Standing Committee on Legal and Constitutional Affairs has recommended that the Australian Government introduce public interest disclosure legislation to provide 'whistleblower' protections in the Australian Government public sector.[67] The Standing Committee recommended that a broad range of Australian Government officials, including officers in intelligence agencies,[68] be able to make public interest disclosures about 'serious matters'[69] to their agency, or to designated external authorities such as the IGIS. A person who makes a public interest disclosure in accordance with the legislation would receive protection including immunity from criminal liability under secrecy offences and administrative sanctions.[70] As discussed in Chapter 2, the recommendations in this Report are premised on the desirability and existence of strong protections for whistleblowers.

8.69 In relation to the second safeguard, the *Australian Security Intelligence Organisation Act 1979* (Cth) includes an exception to the prohibition on disclosure for communications made with the approval of the Director-General of ASIO or an officer having the authority of the Director-General to give such approval.[71] The provisions of the *Intelligence Services Act* include similar exceptions.[72]

8.70 Australia's international obligations under the ICCPR do not only cover the way in which laws are framed, but extend to the way in which those laws are enforced. The Commonwealth Director of Public Prosecutions is required to consider a number of factors before deciding to prosecute a matter, including whether prosecution of the offence is in the public interest. International human rights standards are not expressly included as a factor in the list of matters relevant to determining public interest, but other factors include whether the consequences of a conviction would be unduly harsh

65 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 4.
66 Ibid s 8.
67 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.
68 Ibid, Rec 3; [3.83].
69 Ibid, Rec 7.
70 Ibid, Rec 14.
71 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2)(c).
72 *Intelligence Services Act 2001* (Cth) ss 39(1)(c)(iv), 39A(1)(c)(iv), 40(1)(c)(iv).

or oppressive and the availability and efficacy of any alternatives to prosecution, such as disciplinary or civil proceedings.[73]

8.71 If an individual was prosecuted under one of the AIC secrecy offences, and the power to prosecute was exercised in a way that was inconsistent with the individual's rights under art 19 of the ICCPR, the individual would be able to lodge a complaint with the United Nations Human Rights Committee under the First Optional Protocol to the ICCPR, once all domestic remedies had been exhausted.

8.72 Agencies outside the AIC may obtain or generate information that could, if disclosed without authority, harm national security. The ALRC's view is that the disclosure of this information should be regulated by the general secrecy offence, which makes it an offence to disclose information which did, was reasonably likely to, or was intended to harm national security, defence or international relations of the Commonwealth.

Information obtained or generated by law enforcement agencies

8.73 The unauthorised disclosure of law enforcement information has the potential to prejudice investigations and operations, and, as is the case in witness protection, compromise people's safety. Law enforcement agencies like the Australian Federal Police (AFP) obtain and generate a variety of information, ranging from information that relates to national security and federal offences, protective security services and all policing matters in the Australian Capital Territory.

8.74 Current secrecy offences relating to law enforcement information are fairly broad. For example, s 60A of the *Australian Federal Police Act 1979* (AFP Act) makes it an offence for a police officer to make a record of, or divulge or communicate, information obtained in the course of performing his or her duties under the AFP Act, the *Law Enforcement Integrity Commissioner Act 2006* (Cth) or the *Witness Protection Act 1994* (Cth).

8.75 Secrecy provisions governing the Australian Crime Commission (ACC)—whose role is to collect, correlate, analyse and disseminate criminal information and intelligence and undertake criminal intelligence operations and investigations[74]—and the Australian Commission for Law Enforcement Integrity (ACLEI)—a federal anti-corruption body—similarly cover all information obtained by officers in the course of their duties.[75] These provisions do not include an express requirement that the disclosure of information cause, or is likely or intended to cause, harm.

---

73 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* (2009), [2.10].
74 *Australian Crime Commission Act 2002* (Cth) s 7A.
75 Ibid s 51; *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 207.

8.76 Other offences dealing with the disclosure of law enforcement information are narrower and more targeted. For example, it is an offence for any person to disclose information about the identity or location of a person in the National Witness Protection Program, or information which compromises the security of such a person.[76] Similarly, it is an offence for a person to disclose information that reveals, or is likely to reveal, that a person is using an assumed identity where that disclosure endangers or is likely to endanger the health or safety of any person, or prejudices or is likely to prejudice the effective conduct of an operation.[77] While these offences cover disclosures by 'any person', they are limited to particular information the disclosure of which causes, or is likely to cause, harm.

8.77 Because of the breadth of information obtained or generated by police services, the seriousness of the harm caused by the unauthorised disclosure of information in law enforcement agencies may range from negligible to severe, depending on the nature of the information and the timing and context of the disclosure. In 2008, the New South Wales (NSW) Police Integrity Commission conducted research into the unauthorised disclosure of confidential information by NSW police officers.[78] The research used data sourced from complaints about the conduct of police officers to describe the incidence, detection, characteristics and harms associated with unauthorised disclosures by police officers. The research found that in 54% of cases, the unauthorised disclosure resulted in the compromise of an individual's privacy. As the report notes, the seriousness of this consequence can vary—one instance resulted in an assault. Very few unauthorised disclosures compromised an investigation (3%) or involved criminals evading the law (1%).[79] In six cases, the disclosure was deemed to have resulted only in the 'reputation of the NSW police force being tarnished'.[80]

8.78 By way of comparison, the *Official Secrets Act* takes a harm-based approach to the disclosure of law enforcement information, and makes it an offence for an officer to disclose information that does, or is likely to:

- result in the commission of an offence;
- facilitate an escape from legal custody or the doing of any other act prejudicial to the safekeeping of persons in legal custody; or
- impede the prevention or detection of offences or the apprehension or prosecution of suspected offenders.[81]

---

76 *Witness Protection Act 1994* (Cth) s 22.
77 *Crimes Act 1914* (Cth) s 15XS.
78 J People, *Unauthorised Disclosure of Confidential Information by NSW Police Officers* (2008) NSW Police Integrity Commission.
79 Ibid 21, 26.
80 Ibid 21.
81 *Official Secrets Act 1989* (UK) s 4(2).

Submissions and consultations

8.79 Several law enforcement agencies argued that the secrecy offences governing their agencies should not include an express requirement of harm.

8.80 The AFP, for example, submitted that, because of the nature of their work—including the investigation of serious criminal activity—it is essential that the AFP 'maintain operational security and absolute integrity' of their information. The AFP submitted that because the 'likelihood of harm from disclosure is self-evident', secrecy provisions in the AFP Act should not include an express harm requirement.[82]

8.81 Similarly, the ACC submitted that while harm was not an element of the secrecy offences in the *Australian Crime Commission Act 2002,* the harm of unauthorised disclosure was

> clear from the context which establishes a national criminal intelligence and investigative body authorised to exercise coercive powers in strict secrecy and operate a national criminal intelligence database.[83]

8.82 The ACC submitted that, as is the case with national security intelligence agencies, individual officers may have a limited view of the significance of particular information and are therefore not in a position to judge the harm likely to be caused by its disclosure. The ACC also noted that secrecy laws were necessary to protect information provided to law enforcement agencies under information-sharing arrangements as the agencies need absolute confidence that information will be tightly controlled within an agreed sharing network.[84]

8.83 Other submissions sought to explain why information contained or generated by law enforcement agencies required a high level of protection. For example, ACLEI submitted that:

> 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.[85]

8.84 Some government agencies handle information which, if disclosed, could harm the operations or investigations of law enforcement agencies. For example, AUSTRAC noted that current secrecy offences in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) protect information on the basis that its disclosure

---

82 Australian Federal Police, *Submission SR 70,* 14 August 2009.
83 Australian Crime Commission, *Submission SR 75,* 19 August 2009.
84 Ibid.
85 Australian Commission for Law Enforcement Integrity, *Submission SR 18,* 18 February 2009.

may adversely affect the prevention, detection, prosecution and punishment of criminal offences, the recovery of criminal assets and protection of the national revenue. AUSTRAC submitted that it would not be necessary to extend this approach to *all* information accessed by AUSTRAC officers in the course of their employment. Rather, the secrecy provisions should be limited to a subset of information, the disclosure of which will cause harm of the kinds described.[86]

ALRC's views

8.85 As discussed above, consistency with Australia's international obligations under the ICCPR, laws that infringe on freedom of expression must be necessary and proportionate to the protection of specific public interests.[87] This means that while some information is justifiably subject to close protection, there cannot be an absolute ban on all disclosures.

8.86 In the ALRC's view, s 60A of the AFP Act, which covers all information obtained in the course of performing an officer's duties, is not proportionate to the protection of public interests in public safety and effective law enforcement. In contrast to the 'mosaic' arguments made in relation to information handled by intelligence agencies—that even the unauthorised disclosure of seemingly innocuous information may, when put together with other information, cause harm to national security—the ALRC is not convinced that the disclosure of any and all information handled in the course of a police officer's duties is likely to cause the same degree of harm.

8.87 The ALRC is not persuaded by arguments that an express requirement of harm is inappropriate because of the potential difficulties in proving harm and the possibility that further harmful information might be disclosed during a prosecution. These issues arise in the course of many prosecutions and are commonly dealt with by prosecutors and courts.

8.88 Rather than covering all information obtained or generated by a law enforcement agency, a criminal secrecy offence should attach only to disclosures of information that cause, or are likely to cause harm to law enforcement operations or objectives. The ALRC notes that it is common to describe law enforcement information deserving of protection by criminal sanction in terms of the harms that its disclosure may cause—the secrecy offences in relation to witness protection and assumed identities, noted above, already take this approach, as does the UK *Official Secrets Act*.

8.89 The ALRC therefore considers that secrecy offences relating to law enforcement agencies should generally include an express requirement that the disclosure cause, or is likely or intended to cause, harm to the interests or operations of law enforcement.

---

86 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

87 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976) art 19(3).

This harm is articulated in the recommended general secrecy offence as 'prejudice [to] the prevention, detection, investigation, prosecution or punishment of criminal offences'.[88]

8.90 The ALRC recognises that certain categories of information handled in the law enforcement context are particularly sensitive, and the harm caused by disclosure potentially very serious. The ALRC considers that the current offences that protect information about the identity and location of people in witness protection, or the identity of officers with an assumed identity, are examples of offences that are necessary and proportionate to the protection of essential public interests because they are confined to particular information or framed in terms of the harm caused by the disclosure of that information. Criminal intelligence information handled by the ACC may also warrant special protection akin to information obtained and generated by national security intelligence agencies—with the appropriate safeguards discussed above in relation to those offences.

8.91 Where there is no express harm requirement included as an element of a secrecy offence, it is important to ensure that the category of information covered by the offence is narrowly and clearly defined in order to confine the offence only to information that, by its nature, would cause harm if disclosed without authority.

8.92 The secrecy offences in legislation governing the Australian Defence Force, which are also aimed at protecting essential public interests—namely defence and national security—may provide a useful model for the protection of information held by law enforcement agencies by taking both a harm-based and categories approach. Section 73A of the *Defence Act 1903* (Cth) is confined to particular information. It prohibits a member of the Defence Force or a person engaged under the *Public Service Act 1999* (Cth) from communicating a narrowly defined category of information, being:

> 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.

8.93 At the same time, s 58 of the *Defence Force Discipline Act 1982* (Cth) takes a harm-based approach and makes it an offence for a member or officer of the Defence Force to disclose information where 'the disclosure is likely to be prejudicial to the security or defence of Australia'.

---

88 Recommendation 5–1.

8.94 For other Commonwealth officers who handle law enforcement information, the general secrecy offence will make it an offence to disclose information which causes, is likely to cause, or is intended to cause harm to law enforcement activities and outcomes.

Personal and commercial information

8.95 As summarised in Chapter 3, a large proportion of specific secrecy offences cover personal and commercial information. In Chapter 4, the ALRC expresses the view that the unauthorised disclosure of personal or commercial information does not, without more, warrant criminal sanctions under the general secrecy offence.

8.96 The disclosure of personal and commercial information generally would not attract criminal sanctions in the private sector, unless, for example, fraud was involved. Parity with the private sector is particularly relevant where government agencies compete, or work together, with private business entities, and do not have a regulatory or oversight role. Such agencies can effectively use similar legal mechanisms to protect sensitive personal and commercial information as private sector organisations, such as confidentiality agreements and protections under the general law.

8.97 In addition, other offences protect against the misuse of personal and commercial information by Commonwealth officers. For example, the *Criminal Code* (Cth) makes it an offence for a Commonwealth public official to use information with the intention of dishonestly obtaining a benefit or causing a detriment.[89] At an agency level, the *Privacy Act 1988* (Cth) protects personal information about individuals and establishes rules for handling personal information.

8.98 For these reasons, the ALRC is not recommending that the general secrecy offence cover disclosures that harm personal privacy or commercial affairs. However, the ALRC recognises that this may give rise to the need for separate specific secrecy offences to provide criminal sanctions for the disclosure of personal or commercial information in particular contexts, where the disclosure of such information is likely to cause serious harm to public interests. In developing the reforms to the *Official Secrets Act*—which does not protect against the disclosure of information that harms personal or commercial interests—the UK government also noted that there may be a public interest in protecting private information in some circumstances, such as information provided to government under a statutory requirement.[90]

8.99 Some functions of government require individuals and companies to provide sensitive personal and commercial information to government. For example, laws relating to taxation and social services require individuals to provide government with detailed information about their personal affairs. Other bodies that regulate commercial

---

89 *Criminal Code* (Cth) s 142.2.

90 United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [35].

activities, such as the Australian Prudential Regulation Authority (APRA) and the Australian Securities and Investments Commission (ASIC), require companies to provide information that is commercial-in-confidence.

8.100 Taxation information—that is, information provided by taxpayers pursuant to taxation legislation—is often said to warrant the protection of secrecy offences to encourage willing compliance with taxation laws. The Treasury's review of taxation secrecy provisions states that:

> taxpayers provide this information expecting it to be kept confidential. Compliance with tax laws is more likely if taxpayers know that the information they provide can only be used for limited purposes.[91]

8.101 This view is reflected in the objects clause for the Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth). The first object of the legislation is 'to protect the confidentiality of taxpayers' affairs by imposing strict obligations on taxation officers (and others who receive protected tax information), and so encourage taxpayers to provide correct information to the Commissioner'.[92]

8.102 While there have been some empirical studies into the factors that impact on taxpayers' voluntary compliance with taxation laws, the ALRC has not found any studies dealing with the particular question of the relationship between secrecy offences and voluntary compliance with taxation or other laws. However, Professor Valerie Braithwaite, of the Centre for Tax System Integrity, has conducted an empirical study into the effect of a taxpayers' charter on compliance with taxation laws.[93]

8.103 The *Taxpayers' Charter* sets out 13 principles that govern how officials in the ATO should deal with taxpayers. The principles cover obligations to treat taxpayers fairly and reasonably and as honest in their tax affairs, to provide professional service, explain decisions and to respect taxpayers' rights to complain and seek review of decisions. Relevantly, the *Charter* also includes obligations to respect taxpayers' privacy and keep information confidential in accordance with the law.[94]

8.104 Braithwaite's study found that the *Charter* was a meaningful element in a taxpayer's relationship with the tax office. When taxpayers rated the ATO's

---

91 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 1.

92 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 355-10.

93 V Braithwaite, *Are Taxpayers' Charters 'Seducers' or 'Protectors' of Public Interest? Australia's Experience* (2005) Working Paper 70, Centre for Tax System Integrity.

94 Australian Taxation Office, *The Taxpayers' Charter* <www.ato.gov.au> at 30 November 2009.

performance against the Charter highly, they were cooperative with the authority's demands. In contrast, low Charter ratings led to resistance to regulation.[95]

8.105 While Braithwaite's study found that respect for privacy and confidentiality was an important part of ensuring cooperation, the most important factors influencing high Charter ratings were 'core procedural justice concerns—being treated with respect, as trustworthy, and being consulted in tax related issues'.[96] Confidentiality of taxpayers' information can therefore be seen as one of several factors that encourage the provision of information and voluntary compliance with taxation laws.

Submissions and consultations

8.106 Some government agencies considered that the protection of personal and commercial information by criminal sanctions was integral to their commercial work. For example, Indigenous Business Australia (IBA) submitted that the existence of secrecy provisions

> facilitate IBA's commercial competitiveness with the private sector and enable IBA to perform its commercial functions effectively by creating a high degree of confidence amongst its business partners that information received by IBA will not be subsequently disclosed or published, including under *Freedom of Information* laws.[97]

8.107 The Australian Human Rights Commission submitted that the 'protection of personal information is of utmost importance and [specific secrecy] provisions help to strengthen the integrity of the complaints process'.[98]

8.108 Other government agencies identified areas in which secrecy offences operate in a regulatory environment and argued that including a requirement of harm in these kinds of secrecy offences may weaken the protection of information and compromise the flow of information from a regulated community to the government. Some stakeholders argued that, in this situation, the benefits of including a harm requirement in the offence were outweighed by the public interest in ensuring the free flow of information from regulated entities to regulators, or from individuals to government.[99]

8.109 For example, APRA submitted that a requirement for harm would be inappropriate in the context of the secrecy provision in the *Australian Prudential and Regulatory Authority Act 1998* (Cth) (APRA Act):

> APRA considers that if a requirement to show that a disclosure caused harm were to be adopted in relation to s 56 of the APRA Act then it would weaken in both

---

95 V Braithwaite, *Are Taxpayers' Charters 'Seducers' or 'Protectors' of Public Interest? Australia's Experience* (2005) Working Paper 70, Centre for Tax System Integrity, 23.

96 Ibid, 16–17, 23.

97 Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

98 Australian Human Rights Commission, *Submission SR 61,* 10 August 2009.

99 Social Security Appeals Tribunal, *Submission SR 79,* 24 August 2009; The Treasury, *Submission SR 60,* 10 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; Australian Prudential Regulation Authority, *Submission SR 52,* 6 August 2009.

> perception and reality the protection s 56 affords to regulated entities. Further, APRA staff may not necessarily be in a position to understand the significance of certain information to regulated entities and thus it may be difficult to assess the likelihood of harm to the entity's business, commercial or financial affairs.[100]

8.110 Responding to a similar issue in IP 34, the Australian Bureau of Statistics (ABS) referred to the secrecy offence in the *Census and Statistics Act 1905* (Cth)[101] and submitted that:

> The absolute nature of these provisions is its strength. If an approach were to be adopted that required proof of harm ... it would certainly have the impact of weakening (in both perception and reality) the ABS's ability to maintain the secrecy of identifiable information.[102]

8.111 The ABS argued that without a strong secrecy provision in the *Census and Statistics Act,* the effective production and quality of national statistics would be hindered.[103]

8.112 Similarly, AUSTRAC submitted that:

> From a regulatory perspective, AUSTRAC believes that the perception that the disclosure of information is arbitrary would result in a loss of confidence in the regulator's ability to maintain the confidentiality of commercial information.[104]

8.113 Agencies that rely on the voluntary provision of personal information, such as taxation, health and social security agencies, expressed concern that including a harm requirement would lessen public confidence in their ability to protect personal information.[105] They argued that this in turn could affect voluntary compliance with laws requiring the provision of information. As noted by the Treasury:

> The operation and integrity of the tax system is dependent on voluntary compliance from the public. A cornerstone of this voluntary compliance model is public confidence that confidential information provided to the Government is subject to a high level of protection and may only be used in appropriately limited circumstances.[106]

---

100 Australian Prudential Regulation Authority, *Submission SR 52,* 6 August 2009.
101 *Census and Statistics Act 1905* (Cth) s 19.
102 Australian Bureau of Statistics, *Submission SR 28,* 24 March 2009.
103 Australian Bureau of Statistics, *Submission SR 58,* 7 August 2009.
104 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.
105 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.
106 The Treasury, *Submission SR 60,* 10 August 2009.

8.114 In light of this, the Treasury submitted that 'when dealing with public confidence in the tax system (promoting voluntary compliance), any unlawful release of information is arguably harmful'.[107]

8.115 In addition, FaHCSIA emphasised the importance of maintaining public confidence in the protection of information held in departmental records, and the potential for unauthorised disclosure to erode it:

> This has particular implications for FaHCSIA where personal information about individuals is commonly held. For example, the social security, family assistance and child support laws authorise the collection of sensitive personal information, including information about a person's health, income and assets, and the nature of the person's relationship with their spouse. It is possible that lack of public confidence in the protection of customer's sensitive personal information could lead to attempts to withhold relevant information. Accordingly, FaHCSIA considers that imposing an additional 'harm' requirement to be met in each particular case of unauthorised disclosure would be undesirable.[108]

8.116 Some stakeholders put a contrary view. Civil Liberties Australia, for example, disputed whether the public would lose confidence in the integrity of the system or that the future supply of information would be prejudiced. It submitted that a public harm of this kind was 'incongruent with the purpose of secrecy legislation'.[109]

8.117 The Office of the Privacy Commissioner noted that the 'existence of robust protections around personal information held by government is vital and an important aspect of ensuring community confidence and continued engagement with government'.[110] While the Office considered that 'strong protections must be implemented around the handling and disclosure of personal information held by agencies', it emphasised that sanctions for mishandling personal information should be proportionate:

> The Office suggests that in many instances, administrative penalties could act as a sufficient deterrent against inappropriate handling and disclosure of personal information. However, in the event that an individual suffers harm from a disclosure, the ability for such activity to attract criminal penalties is an important avenue of redress to have available.[111]

8.118 Similarly, Ron Fraser considered that while the need to ensure the future supply of information to government agencies to carry out their functions was an important interest, criminal penalties were not required to achieve this goal. He submitted that administrative penalties and the protection of the general secrecy offence should

---

107 Ibid.
108 Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.
109 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
110 Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009.
111 Ibid.

provide sufficient reassurance to individuals and bodies that provide information to government.[112]

ALRC's views

8.119 The ALRC considers that the unauthorised disclosure of personal or commercial information held by government has the potential to cause harm to private interests, but, in some regulatory contexts, it may also impact on essential public interests. In these circumstances, the harm of the unauthorised disclosure may be better characterised as harm to the ability of the regulatory agency to effectively perform its regulatory function.

8.120 It is an important part of the relationship between citizens and government that if a person or entity provides government with sensitive personal or commercial information, government will protect the information from misuse and unauthorised disclosure. This is particularly important where regulators require sensitive information from individuals and entities, as in the case of the ATO, Centrelink and corporate regulators, and where large amounts of personal and commercial information are collated, as in the case of the ABS. This is recognised, for example, in the *Privacy Act 1988* (Cth) which protects personal information about individuals.

8.121 While an isolated unauthorised disclosure is unlikely to affect the voluntary provision of information, a culture in which sensitive personal and commercial information is not treated with strict confidence by government could undermine essential public interests in effective regulation. However, as noted by the submission from the ATO quoted above, including this kind of harm as an express element of a criminal offence could make the offence unworkable.

8.122 Therefore, the ability to impose criminal penalties for the unauthorised disclosure of personal or commercial information in certain regulatory contexts is necessary to support community confidence in the ability of government to protect the information. The ALRC does not, however, consider that all current secrecy provisions in every regulatory agency are necessary to achieve this purpose—each secrecy provision should be examined in accordance with the ALRC's recommended framework. The ALRC recognises that there is a fine line between the protection of personal and commercial information in regulatory contexts with criminal sanctions and the perceived need to protect information in order to maintain public confidence in, and compliance with, other government activities. If this argument is taken too far, there is a risk that the 'culture of secrecy' in government will remain unchanged.

---

112 R Fraser, *Submission SR 78,* 21 August 2009.

8.123 In the ALRC's view, individuals in agencies that operate in commercial contexts and do not have a regulatory role should not generally be subject to criminal sanctions for the disclosure of personal or commercial information. In these contexts, personal and commercial information should be protected in the same way that the individuals and organisations with which such agencies interact protect information of this kind—that is, through the imposition of disciplinary sanctions and the use of contractual and general law remedies.

8.124 The ALRC considers that specific secrecy offences may be appropriate in some limited circumstances where the disclosure of personal or commercial information may cause harm to important regulatory activities of government. Further, such secrecy offences need not include an express requirement that the disclosure cause harm to a specified public interest.

8.125 Unlike the ALRC's recommended approach to the categories of information obtained or generated by intelligence agencies (where *any* information obtained or generated by these agencies should be subject to secrecy offences), secrecy offences in taxation or social security laws, or laws relating to regulatory bodies, should not be expressed in such broad terms. The category of information protected should be narrowly defined, so that the secrecy provision is not so wide as to cover information that would not harm the regulatory functions of the agency.

8.126 For example, the definition of 'protected information' for the purposes of the proposed taxation secrecy laws is confined to information disclosed or obtained under a taxation law which relates to the affairs of an entity and which identifies that entity.[113] Similarly, the information protected by the secrecy provisions in the APRA Act is limited to information disclosed or obtained under, or for the purposes of, a prudential regulation framework law and relating to the affairs of a regulated entity or other specified bodies. Therefore, the definition of protected information would not include information relating to the policies, governance or administration of the agency.[114]

Other categories of information

8.127 In developing the recommended general secrecy offence, the ALRC has identified four public interests that it considers warrant protection by that provision.[115] However, as the preceding discussion demonstrates, there may be a need for specific secrecy offences to address other harms not included in the general offence.

8.128 This section examines three other categories of information the protection of which may justify criminal sanctions, but which are not covered by the general secrecy

113 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 355-25.
114 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
115 Recommendation 5–1.

offence. The categories discussed are Indigenous sacred or sensitive information, and cockpit voice recordings and telecommunications interception information. However, these categories do not exhaust the categories of information that may warrant protection by specific secrecy provisions.

Indigenous sacred or sensitive information

8.129 The ALRC has identified two criminal secrecy provisions relating to the unauthorised disclosure of Indigenous sacred or culturally significant information.[116] The provisions make it an offence for an officer of the Indigenous Land Corporation to disclose information that is considered sacred or otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders if the disclosure would be inconsistent with the views or sensitivities of those persons.

8.130 In a submission to this Inquiry, IBA submitted that culturally sensitive information, such as information about Indigenous sacred sites, should remain protected by secrecy provisions.[117] Other inquiries into the protection of Indigenous traditional knowledge have noted that Indigenous peoples are concerned about the unauthorised use and reproduction of secret or sacred material for commercial purposes, resulting in the disclosure of information to those not authorised to know or view it.[118] Article 31 of the *Declaration of the Rights of Indigenous Peoples* in part provides that 'Indigenous peoples have the right to maintain, control, protect and develop their cultural heritage, traditional knowledge and traditional cultural expressions'.[119]

8.131 The ways in which Indigenous cultural information may be shared, and to whom it may be transmitted, are of great importance to some Indigenous peoples. For example, under some traditional laws and customs, certain information may be disclosed only to a defined category of people—for example, the women of a particular Indigenous group.[120] In addition, it may be contrary to the traditional laws and customs of an Indigenous group to broadcast the name or image of an Indigenous person who is deceased.

---

116 *Aboriginal and Torres Strait Islander Act 2005* (Cth) ss 193S(3)(b); 193S(3)(d). A number of other secrecy provisions in that Act regulate when Indigenous sacred or sensitive information may be disclosed—for example, in an annual or other reports (ss 144ZB(4), 196(2)) or material laid before Parliament (ss 151, 191L). In addition, the *Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989* (Cth) s 41 prohibits the Institute from disclosing information where it would be inconsistent with the views or sensitivities of relevant Aboriginal persons or Torres Strait Islanders.

117 Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

118 T Janke, *Our Culture: Our Future Report on Australian Indigenous Cultural and Intellectual Property Rights* (1998), 19.

119 *Declaration on the Rights of Indigenous Peoples*, GA Res 61/295, UN Doc A/RES/47/1 (2007) art 31.

120 See, eg, *Wilson v Minister for Aboriginal and Torres Strait Islander Affairs* (1996) 189 CLR 1.

8.132 There are several kinds of harms that may arise from the misuse or unauthorised disclosure of Indigenous information. Because cultural knowledge and traditions are such an important part of Indigenous identity, fracturing traditional information-sharing processes has the potential to 'threaten the cohesiveness and security of an Indigenous group'.[121] The damage caused by the inappropriate disclosure of Indigenous sacred and sensitive information is broader than harm to personal privacy—it harms the structure and identity of Indigenous groups. The harm could also be characterised as a failure to recognise the cultural importance of Indigenous information and knowledge—particularly where there has been past misappropriation and misuse of that information.[122]

8.133 However, it is not easy to answer the question whether Indigenous sacred and sensitive information provided to government requires a criminal offence for its protection. As is the case in many areas of Indigenous law and custom, Australian laws are often unable to protect Indigenous rights and customs adequately. Further, the issue of protection of Indigenous information extends beyond information provided only to government. 'Indigenous sacred and sensitive information' is also a problematic description of the protected information—it is not an agreed or defined term and may encompass a wide variety of material and communications. Acknowledging the difficulties in this area, in *For Your Information: Australian Privacy Laws and Practice,* the ALRC recommended that the Australian government undertake an inquiry to consider whether legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take.[123] This recommendation was not accepted by the Government.[124]

8.134 The ALRC has also made previous recommendations that the *Archives Act 1983* (Cth) and the *Freedom of Information Act* include 'information that, under Indigenous tradition, is confidential or subject to particular disclosure restrictions' as a category of information that may be exempt from disclosure under those regimes.[125] This issue, and the protection of Indigenous information held by government, could be considered as part of an inquiry of the kind recommended by the ALRC. The review or creation of

---

121 E Mackay, 'Indigenous Traditional Knowledge, Copyright and Art—Shortcomings in Protection and an Alternative Approach' (2009) 32(1) *University of New South Wales Law Journal* 1, 3. See also T Janke, *Our Culture: Our Future Report on Australian Indigenous Cultural and Intellectual Property Rights* (1998).

122 T Janke, *Our Culture: Our Future Report on Australian Indigenous Cultural and Intellectual Property Rights* (1998), 19.

123 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 7–2.

124 Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

125 Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Recs 164, 165. Compare, however, Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [10.34] which considered, but did not recommend, a specific exemption in the *Freedom of Information Act 1982* (Cth) for documents that would disclose sensitive Aboriginal and Torres Strait Islander cultural information.

secrecy provisions to protect this kind of information should be developed in consultation with Indigenous peoples, as recommended by the *Declaration on the Rights of Indigenous Peoples*.[126]

Cockpit voice recordings and telecommunications interception information

8.135 A number of specific secrecy provisions make it an offence to disclose on-board recording and cockpit voice recording information without authority.[127] Cockpit voice recording is used to assist investigations into serious aviation incidents. However, as noted in the explanatory memorandum to the Transport Safety Investigation Bill 2002 (Cth):

> [i]t is acknowledged that such recordings constitute an invasion of privacy for the operating crew of an aircraft that most other employees in workplaces are not subject to. Such recordings, therefore, must be treated with the utmost confidentiality and continue to be used for safety investigation purposes only.[128]

8.136 Cockpit voice recording information has been given a high level of protection, to the point that it cannot be used in disciplinary proceedings or as evidence in criminal proceedings against crew members.[129] The risk is that the unauthorised disclosure of cockpit voice recording information could lead to aircrews rendering recording devices inoperative, which would deny access to vital information during safety investigations. These policy considerations would support the retention of secrecy provisions which make it an offence to disclose cockpit voice recording information without authority.

8.137 As with Indigenous sensitive and sacred information, cockpit voice recording information is a category of information that does not easily fall within the general secrecy offence. While the protection of cockpit voice recording information serves the public interest in air safety, it is unlikely that a particular disclosure would, in itself, endanger public safety. The protection of cockpit voice recording information is therefore not amenable to an express requirement of harm, because *any* disclosure, however innocuous, has the potential to compromise the integrity of the systems and procedures for investigating air safety.

8.138 Information obtained by telecommunication interceptions is also subject to strict secrecy offences.[130] Because telecommunications interception involves a serious invasion of a person's privacy, the information has been given a high degree of protection both in Australia and internationally. The UK *Official Secrets Act* makes it an offence for a Crown servant or government contractor to disclose information

---

126 *Declaration on the Rights of Indigenous Peoples*, GA Res 61/295, UN Doc A/RES/47/1 (2007) art 31(2).

127 *Inspector of Transport Security Act 2006* (Cth) s 63(4); *Transport Safety Investigation Act 2003* (Cth) s 53; *Civil Aviation Act 1988* (Cth) s 32AP.

128 Explanatory Memorandum, Transport Safety Investigation Bill 2002 (Cth), 65.

129 *Civil Aviation Act 1988* (Cth) ss 32AQ, 32AR.

130 *Telecommunications (Interception and Access) Act 1979* (Cth) s 63.

obtained through a telecommunications interception or entry and search warrant.[131] It is not necessary to show that the disclosure of this kind of information was 'damaging' in order to prove the offence.[132]

8.139 In this case, the category of information protected is precisely defined, and there are persuasive policy arguments for its absolute protection. On this basis, there is a strong argument that a secrecy offence prohibiting the disclosure of information obtained by way of telecommunications interception does not need to include an express requirement that the disclosure cause, or be likely or intended to cause, harm.

ALRC's views

8.140 In Chapter 4, the ALRC sets out a principled basis for determining the circumstances in which the unauthorised disclosure of government information should attract criminal sanctions over and above any administrative penalties or general law remedies.

8.141 There are three parts to the application of this framework to specific secrecy offences. First, specific secrecy offences should be directed at preventing serious harm to essential public interests.

8.142 Secondly, where a secrecy offence is considered to protect a public interest of sufficient importance to justify the imposition of a criminal sanction, the government should consider the most appropriate way to frame the secrecy offence to ensure that it is confined to disclosures that cause, are likely to cause, or intended to cause, harm to a public interest. Sometimes, this will most effectively be achieved by including an express requirement that, for an offence to be committed, there must be a reasonable likelihood that the disclosure of information will cause harm to a specified public interest.

8.143 While an express requirement of harm is the best approach to ensure that secrecy offences are appropriately confined to disclosures that cause harm to the public interest, the ALRC recognises that, in very limited circumstances, this may not be the most effective way to address the harm caused by the disclosures of some kinds of information. This chapter has examined three key areas that stakeholders have suggested justify specific secrecy offences without an express requirement of harm, because of the sensitivity of the category of information or the needs of particular government agencies.

8.144 The ALRC has come to the view that specific secrecy provisions that govern intelligence agencies need not include an express requirement that a particular

131 *Official Secrets Act 1989* (UK) s 4(3).

132 See *R v Shayler* [2003] 1 AC 247, [11] citing United Kingdom Government Home Office, *Reform of Section 2 of the Official Secrets Act 1911* (1988), [53].

disclosure cause harm. These secrecy offences are directed to protecting the public interest in national security, and the information handled by these agencies is so sensitive that even isolated disclosures of seemingly innocuous information could cause harm.

8.145 Further, the ALRC considers that regulatory agencies, such as taxation, social security and health agencies, and regulatory and oversight bodies such as corporate regulators, need to strictly control disclosures of sensitive personal and commercial information provided to them by the public. For these agencies, the harm caused by the unauthorised disclosure of this information is not only harm to a person's privacy or commercial interests, but harm to the relationship of trust between the government and individuals which is integral to an effective regulatory or taxation system, and the provision of government services. Because this harm may not be concrete enough to prove beyond reasonable doubt in a prosecution for a secrecy offence, the ALRC considers that secrecy offences that seek to protect this kind of information do not require an additional element that the disclosure caused harm.

8.146 Finally, to avoid unnecessary replication of the general secrecy offence, specific secrecy offences should differ in significant and justifiable ways from the recommended general secrecy offence. In other words, specific secrecy offences should be tailored to meet special circumstances not covered by the general secrecy offence—for example, where there is a need to protect an essential public interest that is not protected by the general offence.

8.147 Where there is no express requirement of harm to an essential public interest, or the secrecy offence is not necessary to protect the regulatory functions of government or other essential public interests, it may indicate that the specific secrecy offence is not directed to protecting against harms of the kind that warrant the imposition of criminal sanctions on the individual who discloses that information. Specific secrecy offences of this kind should be considered for repeal.

Recommendation 8–1 Specific secrecy offences are only warranted where they are necessary and proportionate to the protection of essential public interests of sufficient importance to justify criminal sanctions.

Recommendation 8–2 Specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest, except where:

(a) the offence covers a narrowly defined category of information and the harm to an essential public interest is implicit; or

(b) the harm is to the relationship of trust between individuals and the Australian Government integral to the regulatory functions of government.

Recommendation 8–3 Specific secrecy offences should differ in significant and justifiable ways from the recommended general secrecy offence.

9. Specific Secrecy Offences: Elements

Contents

Introduction

9.1 In Chapter 8, the ALRC recommends that specific secrecy offences should be used only where elements of the specific offence differ in significant and justifiable ways from the recommended general secrecy offence.[1] As discussed in that chapter, one way in which specific secrecy offences may differ from the general offence is where it is necessary to impose criminal sanctions for unauthorised disclosures that cause, or are likely to cause, harm to essential public interests not covered by the general secrecy offence. This chapter discusses four other elements of specific secrecy offences—what parties should be regulated; what conduct should be regulated; fault elements; and penalties. This chapter also considers specific subsequent disclosure offences.

1 Recommendation 8–3.

Whose conduct should be regulated?

9.2 Specific secrecy offences currently criminalise the conduct of a range of parties, including:

- Commonwealth officers, whether by referring to all Commonwealth officers, or officers of specific agencies;[2]
- individuals providing services for or on behalf of the Commonwealth;[3]
- individuals engaged in federally funded or regulated areas of the private sector—for example, health service providers[4] and employees of financial institutions;[5]
- state, territory or local government employees;[6]
- individuals assisting in studies or inquiries;[7] or
- 'any person'.[8]

9.3 Some secrecy offences also apply to more narrowly defined groups, such as Pharmaceutical Benefits Scheme prescribers,[9] participants in witness protection programs;[10] and legal practitioners representing persons involved in Australian Crime Commission (ACC) examinations.[11]

9.4 In Chapter 6, the ALRC recommends that the general secrecy offence should apply to current and former Commonwealth officers, which would 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

---

2 See, eg, *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'; *Income Tax Assessment Act 1936* (Cth) s 16 applies to 'a person who is or has been appointed or employed by the Commonwealth or by a State, and who by reason of that appointment or employment, or in the course of that employment, may acquire or has acquired information respecting the affairs of any other person, disclosed or obtained under the provisions of this Act or of any previous law of the Commonwealth relating to income tax'.

3 See, eg, *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.

4 See, eg, *National Health Act 1953* (Cth) s 135AAA.

5 See, eg, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 123.

6 See, eg, *Taxation Administration Act 1953* (Cth) s 13J.

7 See, eg, *Inspector of Transport Security Act 2006* (Cth) s 35(7); *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 4.

8 See, eg, *Aged Care Act 1997* (Cth) s 86-5; *Crimes Act 1914* (Cth) s 3ZQT.

9 *National Health Act 1953* (Cth) s 135AAA(1).

10 *Witness Protection Act 1994* (Cth) s 22(2).

11 *Australian Crime Commission Act 2002* (Cth) s 29B(4).

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 under a Commonwealth contract; and individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth.[12]

9.5 Many existing specific secrecy offences apply to parties other than Commonwealth officers. Therefore, it will be necessary in some circumstances for specific secrecy offences to regulate the conduct of persons other than Commonwealth officers.

9.6 The following section discusses two issues relating to the parties covered by specific secrecy offences—the application of secrecy offences to 'any person'; and the extension of secrecy offences to former, as well as current, Commonwealth officers.

Secrecy offences that apply to 'any person'

9.7 More than 40% of secrecy offences are stated to apply to the handling of information by 'any person'.

9.8 Some specific secrecy offences apply to any person because the information is highly sensitive. For example, the *Intelligence Services Act 2001* (Cth) contains an offence applicable to any person who identifies someone else as being or having been an agent or staff member of the Australian Secret Intelligence Service or who makes public any information from which the identity of such a person could reasonably be inferred, or that could reasonably lead to the identity of such a person being established.[13] The *Australian Security Intelligence Organisation Act 1979* (Cth) contains a similar offence for the disclosure of the identity of an officer of the Australian Security Intelligence Organisation (ASIO).[14] The disclosure of this information could compromise the operations, capabilities and effectiveness of Australia's intelligence, and potentially endanger the life and wellbeing of officers.[15]

9.9 In some instances, secrecy provisions cover any person because the legislation confers a discretion on a Commonwealth officer (usually an agency head) to disclose protected information to, potentially, any person. For example, s 86-5 of the *Aged Care Act 1997* (Cth) makes it an offence for a person to subsequently disclose information obtained under s 86-3 for a purpose other than that for which the information was disclosed. Section 86-3 permits the Secretary to disclose protected information to a number of people, including:

---

12 Recommendation 6–1.
13 *Intelligence Services Act 2001* (Cth) s 41.
14 *Australian Security Intelligence Organisation Act 1979* (Cth) s 92(1).
15 Australian Intelligence Community, *Submission SR 37,* 6 March 2009.

> (a) 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; and ...
>
> (e) if the Secretary believes, on reasonable grounds, that disclosure is necessary to prevent or lessen a serious risk to the safety, health or well-being of a care recipient—to such people as the Secretary determines, for the purpose of preventing or lessening the risk.

9.10 Other secrecy offences are expressed to cover any person present at an examination, or, for example, subject to a confidentiality order issued by an authority.[16] In addition, secrecy provisions that create ancillary offences such as soliciting, obtaining or offering to supply protected information usually cover any person, again reflecting the fact that any person can engage in this kind of conduct.[17]

9.11 There are, however, some offences that, although expressed to apply to any person, may in practice apply only to Commonwealth officers. For example:

- *Development Allowance Authority Act 1992* (Cth) s 114 is expressed to apply to 'a person' who has commercial-in-confidence information 'only because of performing duties or functions' under the Act;

- *Student Assistance Act 1973* (Cth) s 351 is expressed to apply to 'a person', but the information protected by the offence is limited to information obtained for the purposes of certain legislation and held in the records of specific agencies;[18] and

- *Agricultural and Veterinary Chemicals Code Regulations 1995* (Cth) reg 69 is expressed to apply to 'a person', but the information protected by the offence is limited to records made and held by the Australian Pesticides and Veterinary Medicines Authority, a Commonwealth body.

9.12 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC noted that the language used in some secrecy offences, and the practical context in which they operate, mean that the offences will apply mainly to Commonwealth officers—even if the offences are stated to apply to any person.[19] The ALRC proposed that 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', as defined in the

---

16 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 90; *Maritime Transport and Offshore Facilities Security Act 2003* (Cth) s 40; *Productivity Commission Act 1998* (Cth) s 53.

17 See, eg, *Social Security (Administration) Act 1999* (Cth) ss 205, 206; *Health Insurance Act 1973* (Cth) s 130(14), (21); *Child Care Act 1972* (Cth) ss 12K, 12Q. Conduct covered by secrecy offences is discussed later in this chapter.

18 *Student Assistance Act 1973* (Cth) ss 353, 3(1) (definition of 'protected information').

19 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), [10.79].

general secrecy offence, leaving other parties to be governed by the proposed general subsequent disclosure offence.[20]

Submissions and consultations

9.13 Civil liberties groups supported the proposal to review specific secrecy provisions that apply to 'any person'.[21] For example, Civil Liberties Australia (CLA) considered that the application of some secrecy offences 'casts too wide a net', and that:

> The duties of Commonwealth officers are entirely different to ordinary citizens and CLA advocates the restriction of most specific secrecy provisions to Commonwealth officers.[22]

9.14 However, the Australian Government Attorney-General's Department (AGD) noted that in the report, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), the House of Representatives Standing Committee on Legal and Constitutional Affairs recommended that information should be protected at every point in the 'distribution chain', including where that information is handled outside the Commonwealth public sector.[23] The AGD submitted that:

> There is an increasing incidence of information sharing among Commonwealth departments and agencies, as well as with state and territory governments and the private sector. There is a recognised, legitimate need for certain Commonwealth information to be protected through the use of criminal law offences. Accordingly, it would seem appropriate for criminal sanctions to be available to protect sensitive Commonwealth information when it leaves the hands of Commonwealth officers. AGD considers that there is a gap in the protection provided under Commonwealth criminal law to Commonwealth information when it is shared outside of the Commonwealth.[24]

9.15 Many Australian Government agencies explained why particular secrecy offences needed to apply to parties other than Commonwealth officers.[25] For example,

---

20 Ibid, Proposal 10–3. The general secrecy offence is discussed in Chs 5, 6 and 7, while subsequent disclosure offences are discussed in Ch 6.

21 Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

22 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

23 Attorney-General's Department, *Submission SR 67,* 14 August 2009; 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].

24 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

25 See, eg, Australian Crime Commission, *Submission SR 75,* 19 August 2009; Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; 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.

in response to the Issues Paper, *Review of Secrecy Laws* (IP 34),[26] the Department of Human Services (DHS) submitted that it is important that persons other than Commonwealth officers, including individuals in state governments, non-government organisations and the private sector who handle 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.[27]

9.16 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).[28]

9.17 The Australian Taxation Office (ATO) also emphasised the importance of secrecy offences in regulating 'all persons who come into contact with protected information in the course of their employment or in performing services for the Commonwealth'.[29]

9.18 The Australian Transaction Reports and Analysis Centre (AUSTRAC) explained that it was important for secrecy offences in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) to regulate a wider range of people than Commonwealth officers:

> The secrecy provisions of the AML/CTF Act regulate the disclosure of AUSTRAC information by Commonwealth officers, state and territory government officials and persons, and reporting entities in respect to suspicious matter reports. AUSTRAC believes that it is important that state and territory government officials that have access to AUSTRAC information should be subject to the same provisions as Commonwealth officers, as it is the nature of the information that causes harm rather than the source of the disclosure.[30]

9.19 Similarly, the ACC stated that:

> sanctions for breach of secrecy/confidentiality requirements under the ACC Act need to extend to a range of non-Commonwealth figures, including State/Territory participants in ACC task forces and witnesses at ACC examinations, if they are to operate effectively.[31]

---

26 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).
27 Department of Human Services, *Submission SR 26,* 20 February 2009.
28 Ibid.
29 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
30 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.
31 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

9.20 The ACC also provided the example of non-publication directions issued to people present during ACC examinations, such as ACC personnel, witnesses and their legal representatives.[32] The ACC noted that secrecy provisions of this kind needed to cover any person, 'since disclosure of the substance of an examination by a witness may be as harmful as disclosure by a law enforcement officer'.[33]

9.21 The Treasury submitted that 'secrecy provisions should be drafted in a manner that, as clearly as possible, identifies the group of people whose actions that particular secrecy provision seeks to control'.[34] The Treasury explained the approach taken in the proposed new tax secrecy laws:[35]

> In the Tax Secrecy Bill, the first of three offence provisions is clearly defined to apply to 'taxation officers' (effectively a subset of the proposed definition of 'Commonwealth officers'). The offence provision dealing with those entities that are in receipt of information as a consequence of a breach of the law, in our view, correctly refers to all entities (recognising that there are effectively no bounds on the types of entities that can be in receipt of information unlawfully). With respect to the 'lawful' on-disclosure offence provision ... this also refers broadly to 'other people' (while most lawful recipients of taxpayer information will be other Commonwealth officers this will not always be the case—notably, tax secrecy provisions permit the disclosure of information to state and territory tax officers).[36]

ALRC's views

9.22 The ALRC recognises that, in some cases, a secrecy offence may need to apply to any person—for example, where 'any person' could receive protected information, or be subject to a confidentiality order. However, where a specific secrecy offence applies expressly or in practice only to Commonwealth officers, as defined for the purposes of the general secrecy offence, the Australian Government should consider whether it would be sufficient to rely on the recommended general secrecy offence. In addition, where a specific secrecy offence regulates the behaviour of individuals other than Commonwealth officers, the provision should be drafted so as to clearly identify the regulated group.

Recommendation 9–1 Specific secrecy offences that apply to individuals other than Commonwealth officers should clearly identify the parties regulated by the offence.

---

32 *Australian Crime Commission Act 2002* (Cth) s 25A(9).
33 Australian Crime Commission, *Submission SR 75,* 19 August 2009.
34 The Treasury, *Submission SR 60,* 10 August 2009.
35 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth).
36 The Treasury, *Submission SR 60,* 10 August 2009.

Former Commonwealth officers

9.23 Approximately 65% of specific secrecy offences that regulate Commonwealth officers also apply to former Commonwealth officers. This is most commonly done by specifying that the offence applies to a person who is, or has been, an officer or employee of a particular agency.[37]

9.24 The application of s 70 of the *Crimes Act 1914* (Cth) may also extend the application of statutory secrecy provisions to former officers. For example, 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).

9.25 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*[38] 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 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.

9.26 The recommended general secrecy offence covers former as well as current Commonwealth officers.[39] In DP 74, the ALRC proposed that specific secrecy offences that apply to Commonwealth officers should be reviewed to establish whether the offences should apply to both former and current Commonwealth officers.[40]

Submissions and consultations

9.27 Those stakeholders who commented on this proposal supported such a review,[41] echoing submissions made in response to IP 34 that specific secrecy offences should

---

37 See, eg, *AusCheck Act 2007* (Cth) s 15; *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(2); *Environment Protection (Alligator Rivers Region) Act 1978* (Cth) s 31(1).

38 *Archives Act 1983* (Cth) s 9.

39 Recommendation 6–1.

40 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 10–4.

41 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

generally extend to former Commonwealth officers.[42] The Australian Prudential Regulation Authority (APRA) summarised some reasons for ensuring that secrecy offences cover former officers:

> 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.[43]

9.28 Similarly, the ATO commented that, in the taxation context, it is necessary to regulate former officers so that taxation information remains protected even when the person ceases to be a taxation officer.[44]

9.29 As noted by the ACC:

> Although time may reduce the potential for disclosures by a former officer to prejudice public interests, it would normally be appropriate to protect such interests by making secrecy provisions applicable to former Commonwealth officers.[45]

ALRC's views

9.30 The ALRC considers that specific secrecy offences should generally cover both former and current Commonwealth officers. Covering former officers in specific secrecy offences is particularly important because there is no administrative disciplinary framework applicable to them.[46]

9.31 In Chapter 4, the ALRC recommends that s 70 of the *Crimes Act* be repealed and replaced with a new general secrecy offence. Unlike s 70, the recommended new secrecy offence would not operate to extend specific secrecy offences to former Commonwealth officers, as discussed above. If s 70 of the *Crimes Act* is repealed, it will be necessary for those specific secrecy offences to be amended to apply expressly to both current and former officers.

---

42 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.

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

44 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

45 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

46 The protection of information held by former Commonwealth officers is discussed in Ch 13.

9.32 This recommendation may, in some cases, represent an extension of the circumstances in which a person who discloses government information is subject to criminal sanction. The ALRC notes, however, that the majority of specific secrecy offences applicable to Commonwealth officers apply to both former and current officers. In addition, this recommendation must be considered in the context of the other recommendations in this Report intended to ensure that specific secrecy offences are retained or enacted only where disclosures are reasonably likely to cause harm to essential public interests.[47]

Recommendation 9–2 Specific secrecy offences that apply to Commonwealth officers should also apply to former Commonwealth officers.

What conduct should be regulated?

9.33 In Chapter 6, the ALRC recommends that the general secrecy offence should cover only the 'disclosure' of information.[48] As discussed in Chapter 3, 85% of secrecy offences prohibit disclosing, divulging or communicating Commonwealth information. In addition, approximately 60% of secrecy offences cover conduct other than—and usually in addition to—the disclosure of information, including unauthorised soliciting,[49] receipt or possession of information,[50] as well as obtaining,[51] making a record of,[52] or using[53] information.

9.34 For example, the majority of taxation secrecy provisions refer to both the disclosure and recording of taxpayer information.[54] The Exposure Draft Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill (Tax Laws Exposure Draft Bill) proposes that it would be an offence to disclose or 'make a record' of taxation 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'.[55] 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

47 As defined, Ch 1, essential public interests are those that are sufficiently significant to warrant protection through criminal secrecy offences.
48 Recommendation 6–3.
49 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 165.
50 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9(2); *Crimes Act 1914* (Cth) ss 79(4)–(6), 83.
51 See eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 163.
52 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.
53 See, eg, *Aged Care Act 1997* (Cth) s 86-5.
54 See, eg *Taxation Administration Act 1953* (Cth) s 8XB; *Income Tax Assessment Act 1936* (Cth) s 16(2).
55 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), 24.

> disclosed that information, she has still committed an offence through the recording of the information.[56]

9.35 Section 79 of the *Crimes Act* also imposes criminal sanctions for conduct other than disclosure. As noted in Chapter 3, s 79 protects three categories of information. Two categories relate to information that could be described as defence and national security information, namely information:

- made or obtained in contravention of s 91.1 of the *Criminal Code* (Cth) (ie, by espionage) or pt VII of the *Crimes Act* (ie, in contravention of s 79 itself, or by 'unlawful soundings' prohibited by s 83); or

- relating to a prohibited place or anything in a prohibited place.[57]

9.36 Section 79 criminalises a range of conduct other than disclosure in relation to this information, including where a person:

- retains information when he or she has no right to retain it or when it is contrary to his or her duty to retain it;[58]

- fails to comply with a direction given by a lawful authority with respect to the retention or disposal of the information;[59]

- fails to take reasonable care of the information or to ensure that it is not communicated to a person not authorised to receive it or so conducts him or herself as to endanger its safety;[60] and

- receives 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) or (3) of the *Crimes Act.*[61]

9.37 The espionage offences in s 91.1 of the *Criminal Code* also cover conduct other than disclosure. It is an offence to make, obtain or copy a record of information concerning the Commonwealth's security or defence, or the security or defence of another country.[62] Espionage offences differ from s 79 of the *Crimes Act* in that it is an

---

56 Ibid, 24.
57 *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.
58 *Crimes Act 1914* (Cth) ss 79(2)(b), 79(4)(a).
59 Ibid ss 79(2)(c), 79(4)(b).
60 Ibid s 79(4)(c).
61 Ibid ss 79(5), 79(6).
62 *Criminal Code* (Cth) ss 91.1(3), 91.1(4).

aspect of the offences that the information be communicated, or intended to be communicated, to another country or organisation.

Case study: *R v Dowling*[63]

Simon Lappas was an Intelligence Analyst with the Defence Intelligence Organisation (DIO). He had a security clearance which allowed him to access information classified as 'Top Secret'.

Lappas had visited Sherryll Dowling, a prostitute, on several occasions. On one occasion, Lappas gave Dowling two copies of an intelligence document for her to attempt to sell to a foreign power. They made several unsuccessful attempts to sell the documents, but then informed the DIO of what he had done. The documents were recovered from Dowling's home.

Dowling pleaded guilty to two offences against s 79 of the *Crimes Act* of receiving information knowing or having reasonable ground to believe, that the information was communicated in contravention of the espionage offences in the *Criminal Code*, or the official secrets offences in s 79 of the *Crimes Act*.

In sentencing, Gray J found that Dowling's actions did not involve 'espionage intent'. He considered that Dowling did not seek the documents, nor was she involved in planning to sell the documents; 'rather, they were pressed upon her'. Dowling was convicted and released on condition that she pay a $2,000 bond to be on good behaviour for a five year period.[64]

9.38 As discussed in Chapter 6, some activities, where they are ancillary to a primary offence, will be covered by provisions in the *Criminal Code* which extend criminal responsibility to a person who attempts, aids, abets, counsels, procures or urges the commission of an offence.[65] For example, the offence of incitement may apply where a third party solicits the unauthorised disclosure of information from a Commonwealth officer.[66]

9.39 Further, other provisions of the *Criminal Code* may apply to some unauthorised uses of Commonwealth information. For example, the use of official information with the intention of dishonestly obtaining a benefit or causing a detriment to another person

63 Transcript of Proceedings, *R v Dowling*, (Supreme Court of the Australian Capital Territory, Gray J, 9 May 2003).

64 Ibid. Lappas was convicted of offences against ss 78(1)(b) and 79(3) of the *Crimes Act 1914* (Cth). Section 78(1)(b) has since been repealed and a similar offence enacted in s 91.1(4) of the *Criminal Code* (Cth). On appeal, he was sentenced to two years imprisonment for the offence against s 78(1)(b) and six months for the offence against s 79(3): *R v Lappas* (2003) 152 ACTR 7.

65 *Criminal Code* (Cth) pt 2.4.

66 Ibid s 11.4.

is covered by the provisions dealing with abuse of public office.[67] Unauthorised access to, or modification of, data held in a Commonwealth computer is also the subject of existing offence provisions.[68]

9.40 In DP 74, the ALRC proposed that 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, without justification[69] on the basis that the harm involved in such conduct is not immediately obvious, and administrative action may provide an adequate sanction in such circumstances.[70]

9.41 Recognising that, in relation to defence and security information, there is a risk that conduct other than disclosure could cause harm to essential public interests, the ALRC also proposed a new offence to be included in the *Criminal Code* making it an offence for a person, without lawful authority and intending to prejudice the Commonwealth's security or defence, to:

- disclose or obtain information concerning the Commonwealth's security or defence; or

- 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.[71]

Submissions and consultations

Conduct other than disclosure

9.42 Some stakeholders agreed that secrecy provisions should focus on disclosure alone.[72] A number of stakeholders expressed the view that the mere receipt of information should not attract criminal sanctions.[73] In submissions on IP 34, other stakeholders commented that it may be sufficient to proscribe disclosure, rather than other aspects of information handling.[74] In this context, the DHS noted that:

---

67 Ibid s 142.2.
68 Ibid ss 477.1, 478.1.
69 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 10–5.
70 Ibid, [10.94].
71 Ibid, Proposal 12–2.
72 Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
73 L McNamara, *Submission SR 51,* 6 August 2009; Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009; Law Council of Australia, *Submission SR 30,* 27 February 2009; The Treasury, *Submission SR 22,* 19 February 2009; Australian Press Council, *Submission SR 16,* 18 February 2009.
74 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.

> 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.[75]

9.43 However, some government agencies submitted that conduct other than disclosure may cause harm in certain circumstances, and should be subject to criminal sanction. Commenting on the discussion in IP 34, 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.[76]

9.44 In response to the proposal in DP 74, a number of government agencies argued that specific secrecy offences in their areas of responsibility should extend to conduct other than disclosure of information.[77] For example, the ATO submitted that taxation secrecy offences should extend to conduct such as accessing, making a record of, or receiving protected information:

> The ATO firmly believes that it is necessary to maintain this level of protection over such conduct because it should be considered to be just as inappropriate to access a taxpayer's record, out of mere personal interest ... as it is to record or disclose information. Indeed, making a record of a person's income information may indirectly result in a disclosure of that information (if the record is misplaced) and, as such, this conduct should be regulated in the same manner as disclosures.[78]

9.45 The Treasury noted that 'criminalising the unauthorised recording of information acts as a strong deterrent', and that such offences were important 'given the vast amount of information held by the Tax Office'.[79]

9.46 The Australian Federal Police (AFP) made a similar argument with respect to their area of operation, submitting that:

> The AFP Act regime operates in a context in which it is appropriate to criminalise making a record of prescribed information. Creating unauthorised records of information creates a serious risk of compromise to AFP information holdings. This risk is unacceptable given our role, functions and responsibilities within Government and the community.[80]

---

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

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

77 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Australian Intelligence Community, *Submission SR 77,* 20 August 2009; Australian Crime Commission, *Submission SR 75,* 19 August 2009; Australian Federal Police, *Submission SR 70,* 14 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009; The Treasury, *Submission SR 60,* 10 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

78 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

79 The Treasury, *Submission SR 22,* 19 February 2009.

80 Australian Federal Police, *Submission SR 70,* 14 August 2009.

9.47 The ACC disagreed with the proposal that specific secrecy offences should generally cover only the disclosure of information. The ACC expressed concern that 'this approach risks creating a position where a person detected preparing to make a disclosure, but not yet attempting to do so, may not be subject to a criminal sanction':

> When dealing with information that may represent a risk to personal safety, it is desirable to be able to intervene at any point in the disclosure and onward disclosure process so as to prevent harm from being done. Such intervention would be of limited effectiveness if it could not be backed up by sanctions.[81]

9.48 With respect to social security and family assistance laws, the Department of Families, Housing, Community Services and Indigenous Affairs (FaHCSIA) considered that it was important that secrecy offences continue to apply to unauthorised access to information and suggested that the term 'obtaining' might best describe the prohibited conduct.

> FaHCSIA accepts that, in many cases, it may not be appropriate to impose a criminal penalty on a person who receives, or is in possession of protected information, particularly where they have received the information without soliciting it. However, the term 'obtaining' is capable of referring to someone being proactive in acquiring the protected information. It is appropriate for criminal liability to attach to a person who knowingly obtains protected information for unauthorised purposes.[82]

Proposed security offence

9.49 In relation to the ALRC's proposed re-working of s 79 of the *Crimes Act,* the AGD expressed some concerns that the proposed security offence did not cover some conduct currently included in s 79, such as the retention of information, failure to comply with a lawful direction, failure to take reasonable care, and receipt of protected information. The AGD considered that these provided 'an important protection against espionage and other unlawful access to information' and their omission may result in weakening protection for national security information:

> For example, if someone fails to comply with a lawful direction about storage of information, this could mean the information is vulnerable to those who might seek to obtain the information unlawfully.[83]

9.50 The AGD supported placing higher obligations on people who have access to this kind of information:

> In view of the damage that could be caused, it is important that those who have access to such information are vigilant in ensuring it is appropriately protected at all times. Given that people who have access to such information will generally have been

---

81 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

82 Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.

83 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

> required to go through a rigorous security clearance process and security awareness training, it is reasonable that they be subject to these higher standards of care with respect to certain information.[84]

9.51 Other stakeholders argued that a security offence was unnecessary, given the scope of the proposed general secrecy offence, which would make it an offence to disclose information that caused, or was likely or intended to cause, harm to national security or defence.[85]

9.52 In response to IP 34, the Australian Intelligence Community (AIC) commented on the espionage offences in s 91.1 of the *Criminal Code,* which prohibit making, obtaining or copying certain 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.[86]

ALRC's views

9.53 In accordance with the ALRC's framework for the reform of secrecy provisions, specific secrecy offences should be confined to circumstances where they are necessary to protect essential public interests.[87] The ALRC considers that, in most cases, harm is only likely to be caused by the disclosure of information, but acknowledges that there may be contexts that justify applying criminal sanctions to other conduct.

9.54 For example, the espionage offences in the *Criminal Code* cover conduct other than disclosure, including copying or obtaining information. Importantly, however, these provisions also require an intention to deliver the information to another country or foreign organisation, and an intention to prejudice the Commonwealth's security or defence, or advantage another country's security or defence. In the ALRC's view, these provisions are warranted because they are limited to the national security context and clearly indicate the essential public interest they are seeking to protect.

9.55 Similarly, s 79(2) of the *Crimes Act,* which covers the unauthorised retention of information and the failure to comply with a direction with respect to the disposal or retention of information, require that the person engaging in the conduct act with 'the intention of prejudicing the security or defence of the Commonwealth or part of the Queen's dominions'. However, the other offences in s 79 do not require an intention that the conduct cause harm to security or defence.

---

84 Ibid.

85 R Fraser, *Submission SR 78,* 21 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

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

87 The ALRC's framework for reform of secrecy provisions is set out in Ch 4.

9.56 In the ALRC's view, criminal offences for conduct other than disclosure in relation to security or defence information may be justified by the sensitive nature of the information and seriousness of the damage that may result from the misuse of the information. However, the ALRC considers that these offences should expressly require that the conduct did, or was likely or intended to, damage the security or defence of the Commonwealth.

9.57 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 any harm that may be 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. Where there is an intention to use the information, an ancillary offence, such as aiding and abetting or procuring the commission of an offence, may apply. The *Official Secrets Act 1989* (UK) does not make receipt of official information an offence.

9.58 In the context of law enforcement, it may also be appropriate to impose criminal sanctions for conduct other than disclosure. Again, such offences should include an express requirement that the conduct cause, or is likely or intended to cause, harm to an essential public interest—for example, where the conduct is likely to prejudice the prevention, detection, investigation, prosecution or punishment of criminal offences.

9.59 However, in relation to personal and commercial information, the ALRC is not persuaded by arguments that other conduct—such as accessing or making a record of information—without more, is sufficient to warrant criminal penalty. Although such conduct may be preliminary to unauthorised disclosure, without more this kind of behaviour is properly an internal disciplinary matter and should be dealt with through the imposition of administrative sanctions.

Recommendation 9–3 Specific secrecy offences should not extend to conduct other than the disclosure of information—such as making a record of, receiving or possessing information—unless such conduct would cause, or is likely or intended to cause, harm to an essential public interest.

Fault elements

9.60 The great majority of Commonwealth secrecy offences do not stipulate fault elements attaching to the physical elements in the offence. Where legislation creating an offence does not specify fault elements, the automatic fault elements set out in the *Criminal Code* apply.

9.61 Under the *Criminal Code*, the fault element for a physical element of an offence consisting of conduct is intention.[88] In secrecy offences, the 'conduct' will usually be the disclosure of information. This means that, unless expressly stated otherwise, a person must intend to disclose the information before that disclosure can constitute a criminal offence. Inadvertent disclosure, for example, because a person did not take proper care of information, would not constitute an offence.

9.62 The *Criminal Code* also provides that the fault element for a physical element consisting of a circumstance or a result is recklessness.[89] A person is reckless if he or she is aware of a substantial risk that a circumstance exists, or a result will occur, and, having regard to all the circumstances, it is unjustifiable to take that risk.[90] Under the *Criminal Code*, recklessness is established by proving intention, knowledge or recklessness.[91]

9.63 A 'circumstance' in the context of a secrecy offence might be the nature of the information, for example, that the information disclosed was acquired in the course of a person's duties. A 'result' of conduct proscribed by a secrecy offence might be, for example, that the disclosure of the information caused, or was likely to cause, harm.

9.64 The following sections discuss the fault elements attaching to conduct, circumstances and results in specific secrecy offences.

Fault element attaching to conduct

9.65 As noted above, the fault element for the conduct element of almost all specific secrecy offences is intention. In most cases, this is because no fault element is specified and, therefore, the *Criminal Code* provides that intention is the fault element to be applied.

9.66 Only a few secrecy offences specify that a fault element other than intention applies to the disclosure 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.

88 *Criminal Code* (Cth) s 5.6(1).
89 Ibid s 5.6(2).
90 Ibid s 5.4(1), (2).
91 Ibid s 5.4(4).

9.67 Some specific secrecy offences are strict liability offences. 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 complaint made to the Superannuation Complaints Tribunal. This offence is stated to be an offence of strict liability.[92] This means that the prosecution is not required to prove that the defendant had any particular mental state when committing the offence. The *Criminal Code* provides that defences of mistake of fact, and of intervening conduct or event, are available in relation to strict liability offences.[93]

9.68 Offences of strict liability must be considered in light of the policy position stated in the AGD *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (*Guide to Framing Commonwealth Offences*) that it is generally neither fair, nor useful, to subject people to criminal punishment for unintended actions or unforeseen consequences unless they resulted from an unjustified risk.[94]

9.69 In 2002, the Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) reviewed strict liability offences in federal legislation.[95] The Scrutiny of Bills Committee considered that strict liability may be appropriate in the following circumstances: to ensure the integrity of a regulatory regime; to protect the general revenue; to overcome difficulties in prosecuting fault provisions; and to overcome arguments about the defendant's knowledge of a legislative provision which has been incorporated into the offence.[96] The Scrutiny of Bills Committee recommended that strict liability should apply only where the penalty does not include imprisonment, and where the monetary penalty does not exceed $6,600 for an individual and $33,000 for a body corporate.[97]

9.70 The *Guide to Framing Commonwealth Offences* advises that a strict liability offence is appropriate only if each of the following considerations applies:

- the offence is not punishable by imprisonment and the monetary penalty does not exceed the amount specified by the Scrutiny of Bills Committee;

---

92 *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63(2A). See also *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) ss 175-10, 183-1; *Maritime Transport and Offshore Facilities Security Act 2003* (Cth) s 40; *Agricultural and Veterinary Chemicals Code Regulations 1995* (Cth) reg 69; *Civil Aviation Regulations 1988* (Cth) s 132; *Torres Strait Fisheries Regulations 1985* (Cth) reg 13; *Sex Discrimination Act 1984* (Cth) s 92.

93 *Criminal Code* (Cth) ss 6.1, 10.1.

94 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 24.

95 Australian Parliament—Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002).

96 Ibid, 284–285.

97 Ibid, 284.

- the punishment of offences not involving fault is likely to significantly enhance the effectiveness of the enforcement regime; and

- there are legitimate grounds for penalising persons lacking 'fault', for example, because they will be placed on notice to guard against any possible contravention.[98]

9.71 In Chapter 6, the ALRC recommends that the fault element attaching to the disclosure of information in the general secrecy offence and the subsequent disclosure offences should be intention.[99] In DP 74, the ALRC proposed that specific secrecy offences should generally also stipulate intention as the fault element for the disclosure of information.[100] The ALRC also proposed that specific secrecy offences which provide that strict liability applies to one or all physical elements should be reviewed to establish whether the application of strict liability remains justified.[101]

Submissions and consultations

9.72 A number of stakeholders supported these proposals.[102] For example, Liberty Victoria stated that criminal liability should only attach where there is the requisite mental element and that, in relation to the disclosure of official information, the requisite fault element should be intention.[103] The ATO noted that the Tax Laws Exposure Draft Bill does not apply strict liability to any element of the equivalent offences because it was not considered necessary in the taxation context.[104]

9.73 The ACC, however, favoured extending criminal liability to reckless disclosure in cases where 'foresight could reasonably have been exercised to avoid a disclosure that could harm law enforcement'.[105]

ALRC's views

9.74 The ALRC considers that specific secrecy offences should generally require intention as to the disclosure of information, or other conduct relating to the information. This is consistent with the framing of most existing secrecy offences, and with the policy in the AGD *Guide to Framing Commonwealth Offences*.

---

98 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 25.

99 Recommendations 6–5, 6–6, 6–7.

100 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 10–6.

101 Ibid, Proposal 10–7.

102 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

103 Liberty Victoria, *Submission SR 50,* 5 August 2009. See also Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

104 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

105 Australian Crime Commission, *Submission SR 75,* 19 August 2009. See also Australian Federal Police, *Submission SR 70,* 14 August 2009.

9.75 However, a different fault element, such as recklessness, may be justified in exceptional circumstances. For example, it might be appropriate that Commonwealth officers in specific agencies who handle particularly sensitive information should be subject to a criminal offence when they knowingly engage in conduct involving a substantial and unjustifiable risk that the information will be disclosed. In accordance with the ALRC's recommendations in Chapter 8, the elements of such an offence would need to be necessary and proportionate to preventing harm to an essential public interest.[106]

9.76 In the ALRC's view, secrecy offences should not apply strict liability to physical elements consisting of conduct, such as the act of disclosure. At a minimum, in order to be subject to a criminal secrecy offence, a person should intend, or, in more limited circumstances, be reckless, as to the conduct that constitutes the offence.

Recommendation 9–4 Specific secrecy offences should generally require intention as the fault element for the physical element consisting of conduct. Strict liability should not attach to the conduct element of any specific secrecy offence.

Fault element attaching to harm

9.77 In Chapter 8, the ALRC recommends that, except in very limited circumstances, specific secrecy offences should include a requirement that the disclosure of information cause, or be likely or intended to cause, harm to an essential public interest.[107] In *Criminal Code* terms, a requirement that conduct cause, or be likely to cause, harm would be characterised as a result. As noted above, unless it was specified otherwise, the *Criminal Code* would attach recklessness to this element of the offence.[108]

9.78 An example of an offence that includes an express requirement of harm is s 58 of the *Defence Force Discipline Act 1982* (Cth). That offence provides that strict liability applies to the requirement that the disclosure is likely to be prejudicial to the security or defence of Australia. This means that the prosecution is not required to prove that the accused intended that, knew or was reckless as to whether, the disclosure was likely to be prejudicial to the security or defence of Australia.

106 Recommendations 8–1, 8–2.
107 Recommendations 8–1, 8–2.
108 *Criminal Code* (Cth) s 5.6(2).

9.79 In DP 74, the ALRC proposed that where specific secrecy offences incorporate a harm requirement, recklessness should generally be the fault element for offences punishable by imprisonment for more than a maximum of two years. For other offences, the ALRC proposed that strict liability should apply in relation to the likelihood of harm.[109]

Submissions and consultations

9.80 Some stakeholders supported recklessness as the fault element for harm.[110] For example, the ACC submitted that:

> If a person foresaw the possibility of serious harm but proceeded to disclose the potentially harmful information, they should not be able to avoid responsibility by claiming they did not intend to cause the harm they foresaw. In the case of some forms of harm, such as endangering personal safety, it may even be appropriate to impose constructive foresight of the potential harm.[111]

9.81 In response to IP 34, the AGD commented that the difficulties that arise in proving a fault element usually relate 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.[112]

9.82 Also in response to IP 34, the Australian Securities and Investments Commission submitted that, if a harm test were introduced into secrecy offences, strict liability should be applied because it would be very difficult to prove that a person intended or knew that the disclosure of information was likely to harm a specified public interest.[113]

9.83 However, a number of stakeholders expressed concerns about the application of strict liability to the harm requirement in any context. For example, Liberty Victoria

---

109 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 10–2.

110 Australian Press Council, *Submission SR 62,* 12 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009.

111 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

112 Attorney-General's Department, *Submission SR 36,* 6 March 2009. At the time of writing, 60 penalty units amounted to a fine of $6,600.

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

stated that criminal liability must only attach where there is the requisite mental element,[114] while CLA submitted that:

> Criminal sanctions should not apply, absent intention to cause harm to the specified public interest or clear recklessness to the probability of such harm occurring. There is always a potential for government to utilise criminal sanctions to silence reasonable dissent or to attempt to induce unreasonable conformity within the public sector, especially in situations where an open and transparent approach might involve only trivial harm or mild embarrassment.[115]

9.84 Similarly the Australian Press Council submitted that it is not appropriate to have offences of strict liability in legislation dealing with unauthorised disclosure:

> Strict liability may have a place in internal disciplinary procedures for minor matters or in mechanisms dealing with compensation but it is not appropriate where the offence would result in a criminal conviction ... Before a criminal conviction is 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.[116]

ALRC's views

9.85 In Chapter 6, the ALRC recommends that the fault element attaching to the harm element of the general secrecy offence should be recklessness. That is, the offence will only be committed where information has been disclosed by a Commonwealth officer and the officer knows, intends or is reckless as to whether, the disclosure of the information will harm, or is reasonably likely to harm, one of the public interests set out in Recommendation 5–1.[117]

9.86 Similarly, specific secrecy offences that include, as an element of the offence, that the disclosure cause, or is likely to cause, harm to an essential public interest, should generally require recklessness, knowledge or intention as to the likelihood of harm.

9.87 The application of strict liability to the likelihood that the disclosure cause harm may be justifiable in particular circumstances. For example, the application of strict liability to the harm requirement in s 58 of the *Defence Force Discipline Act 1982* (Cth) may be justified by the seriousness of the harm and the special obligations of military personnel. Where strict liability is applied to the likelihood that the disclosure cause harm, the penalty should be lower than that for an offence which requires recklessness, knowledge or intention as to the likelihood of harm.

---

114 Liberty Victoria, *Submission SR 50,* 5 August 2009.

115 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

116 Australian Press Council, *Submission SR 62,* 12 August 2009.

117 Recommendation 6–6. The four harms included in the recommended general secrecy offence are: damaging the security, defence or international relations of the Commonwealth; prejudicing the prevention, detection, investigation, prosecution or punishment of criminal offences; endangering the life or physical safety of any person; and prejudicing the protection of public safety.

Recommendation 9–5 Specific secrecy offences with an express harm requirement should generally require that a person knew, intended that, or was reckless as to whether, the conduct would cause harm to an essential public interest.

Fault element attaching to the nature of the information

9.88 Specific secrecy offences protect a wide range of information. Often the protected information is defined by how the information was obtained—for example, information obtained in the course of an officer's duties. In *Criminal Code* terms, the nature of the information is a physical element consisting of a circumstance and the automatic fault element attached to the physical element is recklessness.[118]

9.89 Some specific secrecy offences depart from the automatic fault elements in the *Criminal Code* by specifying that strict liability applies to the circumstance of the nature of the information subject to the secrecy offence, for example:

- that the information was disclosed or obtained under or for the purposes of a particular legislative provision;[119] or
- that the information was obtained in the performance of functions or duties under legislation.[120]

9.90 The application of strict liability in such cases means that the prosecution is not required to prove that a person knew or was reckless as to whether, for example, the information was obtained in the performance of functions or duties under particular legislation.

9.91 Other specific secrecy offences expressly require knowledge as the relevant fault element, for example:

- s 114 of the *Development Allowance Authority Act 1992* (Cth) applies to a person who has commercial in confidence information, where the person knows that the information is commercial in confidence; and

118 *Criminal Code* (Cth) s 5.6(2).

119 See, eg, *Public Service Regulations 1999* (Cth) reg 7.6(2A); *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s162(8B); *Child Support (Registration and Collection) Act 1988* (Cth) s 58(3); *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS(3); *Student Assistance Act 1973* (Cth) s 12ZU(4B).

120 See eg, *Public Service Regulations 1999* (Cth) reg 7.6(2A); *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s 162(9A)(a); *Social Welfare Commission (Repeal) Act 1976* (Cth) s 8(2A).

- s 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'.

9.92 The second example applies when a person has actual knowledge that the information was of a particular kind, but also when the person did not actually know, but reasonably should have known. The AGD *Guide to Framing Commonwealth Offences* states that this kind of formulation is an 'attempted compromise between requiring proof of fault and imposing strict liability'. The *Guide* notes that, depending on the context, a court may read in a requirement for the prosecution to prove something akin to recklessness, and recommends that this terminology be avoided.[121]

Submissions and consultations

9.93 In relation to the nature of the information covered by the general secrecy offence, the Commonwealth Director of Public Prosecutions (CDPP) stated that:

> Absolute liability should apply to the 'jurisdictional element' of Commonwealth offences ie the link between the offence and the relevant legislative power of the Commonwealth. This link is also known as the 'Commonwealth connector'. The CDPP considers that the fact that the defendant has or had the information because s/he is or was a Commonwealth officer is the Commonwealth connector in the proposed general secrecy offences and that absolute liability should apply to this element.[122]

9.94 The CDPP also noted that this position is reflected in the *Guide to Framing Commonwealth Offences*, which provides:

> Absolute liability should apply to the jurisdictional element. For example, in the case of theft of Commonwealth property, the act of theft is the substantive element of the offence; while the circumstance that the property belongs to the Commonwealth is a jurisdictional element.[123]

ALRC's views

9.95 The ALRC's approach in this Report is to focus on the harm of disclosure, rather than categories of information. To this end, the ALRC recommends that, except in very limited circumstances, specific secrecy offences should include an express requirement that the disclosure cause, or is likely or intended to cause, harm to an essential public interest.[124]

---

121 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 21.

122 Commonwealth Director of Public Prosecutions, *Submission SR 65,* 13 August 2009.

123 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 25.

124 Recommendations 8–1, 8–2.

9.96 Where there is an express requirement of harm it may be appropriate to attach strict liability to the circumstance that the information was obtained in a particular manner, or is of a particular kind. In these circumstances, the act of disclosing the information reckless as to whether, or intending that, the disclosure cause harm is the substantive element of the offence and the circumstance that the information was 'Commonwealth information' amounts to a jurisdictional element.

9.97 However, where a specific secrecy offence does not include an express requirement of harm, the key requirement for criminal liability is that the information disclosed was of a particular kind, for example, 'taxation information'. For these offences, the ALRC considers that strict liability should not attach to the circumstance that the information falls into a particular category. It is important that, in order to have committed an offence, the person knew, or was reckless as to whether, the information was in the protected category of information.

Recommendation 9–6 Specific secrecy offences without an express harm requirement should require that a person knew, or was reckless as to whether, the protected information fell within a particular category, and should not provide that strict liability applies to that circumstance.

Subsequent disclosure offences

9.98 In Chapter 6, the ALRC recommends the creation of two offences for the subsequent unauthorised disclosure of Commonwealth information: (a) where a person receives the information in confidence; and (b) where a person receives the information knowing that, or reckless as to whether, the information has been disclosed in breach of the general secrecy offence (the general subsequent disclosure offences).[125] In addition, in Chapter 7, the ALRC recommends that any person should be able to apply to the court for an injunction to restrain the disclosure of information in contravention of the general or subsequent disclosure offences.[126]

9.99 A number of specific secrecy offences extend to some form of subsequent disclosure—that is, disclosure by a person who received protected information as a result of a disclosure by a Commonwealth officer or official entity. There are two kinds of subsequent disclosure offences. The majority deal with subsequent disclosure of information legally obtained by a person. A smaller number of offences cover the subsequent disclosure of information obtained as a result of breach of a secrecy law. Because different issues arise in relation to each, they are discussed separately below.

---

125 Recommendations 6–6, 6–7. In Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), only one subsequent disclosure offence was proposed, which applied to information received as a result of an unlawful disclosure: Proposal 8–3.

126 Recommendation 7–6.

Subsequent disclosure of lawfully disclosed information

9.100 Most subsequent disclosure offences cover disclosures by persons who obtain protected information legally—for example, under specific legislative provisions that provide for information to be shared. For example, s 86-5 of the *Aged Care Act* (discussed above) makes it an offence for a person to disclose information given to them by the Secretary for a purpose other than that for which the information was originally disclosed.[127]

9.101 As noted earlier in this chapter, specific secrecy offences may extend to a wide range of people who handle sensitive government information, such as officers in other agencies, contracted service providers and state and territory government employees. Subsequent disclosure offences are one way to ensure that protected information remains protected when shared with others within and beyond the Australian Government.

9.102 Generally, where a secrecy offence includes an offence of subsequent disclosure of information obtained as a result of a lawful disclosure, the penalties for the initial and subsequent disclosure of protected information are the same.[128] In DP 74, the ALRC proposed that 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.[129]

Submissions and consultations

9.103 Several government agencies expressed the view that, in some circumstances, subsequent disclosure offences should extend to the unauthorised disclosure of information obtained lawfully. The AGD noted that the proposed general secrecy offence and accompanying subsequent disclosure offence did not cover the situation in which Commonwealth information is lawfully received by a person who is not a Commonwealth officer and that person discloses the Commonwealth information in circumstances which would otherwise breach the general secrecy offence. The AGD considered that:

> there needs to be an offence for subsequent unauthorised disclosure of information by a third party who has received information lawfully from a Commonwealth officer for a specified purpose. Without this, there will be no protection provided to Commonwealth information under the proposed general secrecy offence where the

127 See also *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E.

128 See, eg, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 121(2), (7), (12); *Aged Care Act 1997* (Cth) ss 86-2, 86-5.

129 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 11–6.

> information was on-disclosed by an individual not covered by the definition of Commonwealth officer.[130]

9.104 AUSTRAC submitted that information, regardless of whether the initial disclosure was authorised or unauthorised, needs to be protected if subsequent disclosure would harm the public interest:

> The subsequent disclosure provisions in the AML/CTF Act prohibit the disclosure of AUSTRAC information except in a limited number of circumstances. The circumstances in which AUSTRAC information could be released include for the purposes of or in connection with an investigation or possible investigation, and for tribunal and court proceedings. This recognises that the harm that might be caused by the disclosure of AUSTRAC information is not lessened by its previous disclosure.[131]

9.105 The DHS submitted 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.[132]

9.106 The Treasury noted that the Tax Laws Exposure Draft Bill regulates the subsequent disclosure of information obtained lawfully, as well as unlawfully:[133]

> Disclosure provisions in the Tax Secrecy Bill seek to clearly identify the circumstances in which taxpayer information can be disclosed, usually in terms of the agency to whom the disclosure can be made and the purpose of that disclosure ... Given that these disclosures are limited to particular purposes, there would be an understandable expectation that these limitations would continue to apply. Otherwise, the initial limitations on disclosure by the ATO would arguably be of little importance.[134]

---

130 Attorney-General's Department, *Submission SR 67,* 14 August 2009.

131 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

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

133 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-155 (subsequent disclosure of information lawfully obtained); sch 1 pt 1 cl 355-265 (subsequent disclosure of information unlawfully obtained).

134 The Treasury, *Submission SR 60,* 10 August 2009.

9.107 Because most lawful disclosures occur between Commonwealth agencies, the Treasury considered that specific secrecy provisions may be more effective in regulating subsequent disclosure by non-Commonwealth officers than the general subsequent disclosure offence:

> While Treasury support the notion that limitations should be applied along 'the chain' of disclosure, it is not clear whether this could meaningfully be applied in a general context. The Tax Secrecy Bill proposes to impose limitations on the on-disclosure of taxpayer information by clearly distinguishing between 'tax officers' and 'non taxation officers' who are in receipt of information lawfully.[135]

ALRC's views

9.108 As noted above, in Chapter 6 the ALRC recommends the creation of two offences for the subsequent unauthorised disclosure of Commonwealth information. One of these offences is framed to apply to the subsequent disclosure of information by a person, who is not a Commonwealth officer, who has received the information on terms requiring it to be held in confidence. This offence is intended to apply to a range of situations in which Commonwealth information is shared lawfully with people who are not Commonwealth officers, where they are aware, or are reckless as to whether, the information should be protected. In addition the person must know, intend, or be 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 Recommendation 5–1.[136]

9.109 The ALRC considers that, in some circumstances, the imposition of criminal sanctions for the subsequent disclosure of information lawfully obtained may also be warranted in specific secrecy offences; in particular, where the offences relate to defined information and include a prescriptive regime for sharing information with particular persons for particular purposes.

9.110 As with all specific secrecy offences, however, subsequent disclosure offences should be confined to unauthorised disclosures of information which would cause, or are likely or intended to cause, harm to essential public interests. This will require that the subsequent disclosure offence include an express requirement that the subsequent disclosure cause, or be likely or intended to cause, harm to an essential public interest, except in the very limited circumstances discussed in Chapter 8.[137] Where the fault elements are the same and similar harm is caused by the conduct, the maximum penalties for both the initial and subsequent unauthorised handling of Commonwealth information should be consistent.

---

135 Ibid.
136 Recommendation 6–7.
137 Recommendation 8–2.

9.111 Where the imposition of criminal sanctions for subsequent disclosure is not warranted, it will be appropriate to protect confidentiality using other means, such as memorandums of understanding, contractual confidentiality clauses and other measures discussed in Chapter 14.

Subsequent disclosure of unlawfully disclosed information

9.112 The ALRC has identified a number of areas in which specific secrecy offences include offences for the subsequent disclosure of information that has been unlawfully disclosed.

Taxation information

9.113 Section 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).

9.114 The Tax Laws Exposure Draft Bill proposes to continue to regulate the subsequent disclosure of unlawfully (as well as lawfully) obtained taxation information. Clause 355-265 of the draft Bill would make it an offence for a person to use or disclose protected information that was disclosed or obtained in breach of a provision of a taxation law.

Health and social security

9.115 A number of legislative provisions in the health and social security area create offences for the subsequent disclosure of protected information. For example, the *National Health Act 1953* (Cth) makes it an offence for a person to use or disclose information that he or she 'knows or ought reasonably to know' was disclosed in contravention of a secrecy provision.[138] The secrecy offence in the *Child Care Act 1972* (Cth), which applies to any person and may therefore extend to subsequent disclosure, takes a different approach, in that it requires that the person 'knows, or is reckless as to whether, the information is protected information'.[139]

9.116 Some offences in this area provide higher penalties for subsequent disclosure than the initial unauthorised disclosure. For example, under the *Health Insurance Act 1973* (Cth), where protected information is disclosed to a person in contravention of s 130, the person is guilty of an offence if he or she subsequently discloses the information to another person where he or she knows, or reasonably ought to know, that the disclosure is in breach.[140] The maximum penalty for this subsequent disclosure

---

138 *National Health Act 1953* (Cth) s 135A(14). Similar offences are contained in the *Private Health Insurance Act 2007* (Cth) s 323-50; *Health Insurance Act 1973* (Cth) s 130(15).

139 *Child Care Act 1972* (Cth) s 12L.

140 *Health Insurance Act 1973* (Cth) s 130(15).

is two years imprisonment,[141] while the officer making the initial unauthorised disclosure is liable only to a fine of $550.[142]

National security and law enforcement

9.117 There are currently no subsequent disclosure offences in the specific legislation governing the AIC. As outlined in Chapter 8, the secrecy offences in the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth) cover disclosures of information prepared by or on behalf of the respective intelligence agencies, and having come to the knowledge of the person by reason of being an officer of, or having entered into a contract or arrangement with, the agency.[143] This offence covers people who receive intelligence information lawfully. It does not cover people who disclose information that was disclosed to them unlawfully.

9.118 Similarly, secrecy offences governing law enforcement agencies, while widely drawn, generally do not include specific subsequent disclosure offences for information disclosed in breach of a secrecy offence.

9.119 In these circumstances, the subsequent disclosure of information unlawfully obtained may be regulated in other ways. For example, s 79 of the *Crimes Act* includes two offences of receiving information, knowing or having reasonable ground to believe that it is communicated in contravention of:

- section 91.1 of the *Criminal Code* or s 79(2) of the *Crimes Act*—which prohibit the disclosure of information concerning security or defence of the Commonwealth or other country, or other information, with the intention of prejudicing the security or defence of the Commonwealth; or

- section 79(3) of the *Crimes Act*—which prohibits the disclosure of prescribed information 'entrusted' to a person by a Commonwealth officer.[144]

9.120 In addition, individuals who subsequently disclose information unlawfully disclosed to them may be liable under ancillary offences in the *Criminal Code,* as the following case study illustrates.

---

141 Ibid s 130(23).
142 Ibid s 130(1).
143 *Australian Security Intelligence Organisation Act 1979* (Cth); *Intelligence Services Act 2001* (Cth) ss 39, 39A, 40.
144 *Criminal Code* (Cth) s 79(5), (6).

Case study: *R v Seivers*[145]

James Seivers was an officer of ASIO. In 2002, he removed documents containing information about the Bali bombings from his workplace and took them to his home. His flatmate, Matthew O'Ryan, provided the information to the media.

The jury found Seivers guilty of breaching s 18(2) of the *Australian Security Intelligence Organisation Act 1979* (Cth), which makes it an offence for a person to disclose information that has come into his or her knowledge by reason of having been an officer of ASIO. O'Ryan was found guilty of aiding, abetting or procuring the commission of the offence committed by Seivers.

Even though the Court considered that the two men had engaged in a 'joint enterprise', the Court imposed a higher penalty on Seivers on the ground that he, as an officer of ASIO, had a greater obligation not to disclose the information.[146]

Submissions and consultations

9.121 Most submissions on this issue were directed to the proposed general subsequent disclosure offence, and are discussed in detail in Chapter 6. However, a number of government agencies highlighted the importance of subsequent disclosure offences to their agencies. For example, the Treasury submitted that provisions such as that in s 8XB of the *Taxation Administration Act* were necessary to protect taxation information and 'continue to be appropriate to ensure the integrity of information and the integrity of authorised chains of disclosure'.[147]

9.122 The AIC submitted that, depending on the nature of any general subsequent disclosure offence, specific subsequent disclosure offences could be added to legislation governing the AIC.[148] The AFP suggested that secrecy offences should cover the 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.[149]

145 *R v Seivers* (Unreported, Reasons for Sentence, Supreme Court of the Australian Capital Territory, Gray J, 10 June 2009).

146 Seivers was sentenced to 12 months imprisonment, with six months served through 24 periods of periodic detention. O'Ryan was sentenced to 12 months imprisonment, with three months served through 12 periods of periodic detention. Both were to be released on recognisance in the sum of $2,000 to be of good behaviour for one year.

147 The Treasury, *Submission SR 22,* 19 February 2009.

148 Australian Intelligence Community, *Submission SR 77,* 20 August 2009.

149 Australian Federal Police, *Submission SR 33,* 3 March 2009.

9.123 The AFP considered that this type of offence was

> 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.[150]

9.124 The Australian Commission for Law Enforcement Integrity (ACLEI) submitted that it is particularly concerned to guard against 'tip-offs' being given to witnesses or persons of interest. In this context, 'the same damage, and sometimes more, can result from a secondary disclosure as it can from the primary disclosure'.[151]

9.125 Finally, as noted in Chapter 6, some stakeholders expressed concerns about criminalising the subsequent disclosure of information unlawfully disclosed at all.[152] For example, CLA did not support either the proposed general subsequent disclosure offence, or specific subsequent disclosure offences:

> Extending secrecy provisions beyond the present confines, particularly to persons who are not Commonwealth officers, raises the issue of how this law could be used in the future to silence reporting of poor governance, maladministration or corruption.[153]

ALRC's views

9.126 The unauthorised disclosure of some kinds of information unlawfully in the hands of third parties has the potential to cause harm to essential public interests. There are persuasive reasons, therefore, to protect it with criminal sanctions.

9.127 However, as discussed in Chapter 6, there are concerns that subsequent disclosure offences have the potential to impact adversely on freedom of expression and could unreasonably curtail the media's ability to discuss matters of public interest. In order to avoid placing a disproportionate restriction on freedom of expression, the ALRC considers that, where a criminal offence regulates disclosure by a third party who has received Commonwealth information by way of unlawful disclosure, several safeguards should be put in place.

9.128 First, the ALRC considers that offences for the subsequent disclosure of information unlawfully disclosed should require that the person knew, or was reckless as to whether, the information was initially disclosed in contravention of a secrecy offence. Secondly, all subsequent disclosure offences should require that the person

---

150 Ibid.

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

152 Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009; Australian Press Council, *Submission SR 62,* 12 August 2009; L McNamara, *Submission SR 51,* 6 August 2009.

153 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

know, intend or be reckless as to whether, the subsequent disclosure of the information would cause, or was reasonably likely to cause, harm to an essential public interest.

9.129 For example, officers in the AIC should know that the information they handle is inherently sensitive, and that any disclosure has the potential to harm national security. Similarly, persons who have entered an arrangement or agreement with an AIC agency should be made aware of the high level of responsibility associated with access to intelligence information. However, a person outside the AIC cannot be expected to have a similar level of knowledge or responsibility.

9.130 This approach reflects the UK *Official Secrets Act*, which requires that a subsequent disclosure of information obtained by way of an unauthorised disclosure must be 'damaging', regardless of whether the initial disclosure offence has a similar requirement. For example, while s 1(1) of the *Official Secrets Act* makes it an offence for a member of the security and intelligence services to disclose any information obtained by virtue of his or her position as a member of the services (without a need to show that the disclosure caused harm), the subsequent disclosure offence requires that the subsequent disclosure cause damage, or that the person making the disclosure knew, or had reasonable cause to believe, that it would be damaging.[154]

9.131 Some existing subsequent disclosure offences have inconsistent fault elements attaching to the circumstances in which information has been disclosed. For example, some apply when a person 'ought reasonably to know' or 'has reasonable grounds to believe' that the information has been unlawfully disclosed to them. As noted above, the AGD *Guide to Framing Commonwealth Offences* characterises these formulations as an 'attempted compromise between requiring proof of fault and imposing strict liability' and recommends that they be avoided.[155] In the ALRC's view, the fault element attaching to this circumstance should be knowledge or recklessness, consistent with the automatic fault element in the *Criminal Code*.[156]

Recommendation 9–7 Offences for the subsequent unauthorised disclosure of information should require that:

(a) the information has been disclosed in breach of a specific secrecy offence;

(b) the person knows, or is reckless as to whether, the information has been disclosed in breach of a specific secrecy offence; and

154 *Official Secrets Act 1989* (UK) s 5(3). The exception to this rule is information obtained as a result of the espionage offence in s 1 of the *Official Secrets Act 1911* (UK): s 5(6).

155 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 21.

156 *Criminal Code* (Cth) s 5.6.

(c) the person knows, intends or is reckless as to whether the subsequent disclosure will harm—or knows or is reckless as to whether the subsequent disclosure is reasonably likely to harm—a specified essential public interest.

Penalties

9.132 The final section of this chapter discusses two issues relating to penalties for the breach of specific secrecy offences: inconsistencies in current penalties for secrecy offences and the development of benchmark penalties for secrecy offences that include a requirement of harm.

Inconsistencies between specific secrecy offences

9.133 Penalties in specific secrecy offences vary widely, from a fine of $110[157] to imprisonment for 25 years.[158] The following table provides a breakdown of the maximum penalties applicable to specific secrecy offences, by percentage of offences identified by the ALRC.[159]

Penalty	**%**
Pecuniary penalty only	10%
Imprisonment for 1 year or less	15%
Imprisonment for 2 years	67%
Imprisonment for 5 years	4%
Imprisonment for 7 years	1%
Imprisonment for 10 years	1%
Imprisonment for 15 years or more[160]	1%

157 *Reserve Bank Act 1959* (Cth) s 79B.
158 *Criminal Code* (Cth) s 91.1.
159 Percentages do not add up to 100 due to rounding.
160 This category includes one offence that allows a judge unfettered discretion with respect to the level of penalty that may be imposed: *Defence Act 1903* (Cth) s 73A attracts a maximum penalty of imprisonment 'for any term' or a 'fine of any amount' or both.

9.134 The House of Representatives Standing Committee on Legal and Constitutional Affairs has expressed the view that 'consistency in the range and expression of penalties in criminal secrecy provisions is desirable', but acknowledged that 'there may need to be some flexibility depending on the sensitivity of the information to be protected'.[161]

9.135 In the course of this Inquiry, a number of stakeholders highlighted inconsistencies in the penalties for the unauthorised disclosure of similar kinds of information in similar contexts.[162] For example, ACLEI noted that inconsistent penalty provisions apply to employees of the ACC and the AFP.[163] These offences provide that:

- the maximum penalty that applies to members and staff of the 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;[164] while

- the maximum penalty applying to members, employees and persons engaged by the AFP for engaging in similar conduct is a term of imprisonment for two years and $13,200 fine.[165]

9.136 ACLEI submitted that the penalty in the *Australian Crime Commission Act 2002* (Cth) should be made consistent with that under the *Australian Federal Police Act 1979* (Cth).[166]

9.137 The DHS also 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* [*2008* (Cth)]). Medicare Australia advises that the information protected under the *Health Insurance Act* and the *Dental Benefits Act* is essentially the same.[167]

---

161 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.

162 See, eg, 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.

163 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.

164 *Australian Crime Commission Act 2002* (Cth) s 51.

165 *Australian Federal Police Act 1979* (Cth) s 60A.

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

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

9.138 The DHS stated that these anomalies are even more noticeable within agencies that are subject to more than one secrecy provision. For example, an officer of Medicare Australia who discloses information protected under the *National Health Act* faces a maximum fine 10 times that of an officer committing the same offence under the *Health Insurance Act*, and only the former attracts a sentence of imprisonment.[168]

> 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.[169]

Inconsistencies with the *Crimes Act*

9.139 Part IA of the *Crimes Act* contains a number of provisions relevant to determining penalties for breach of a federal offence, which apply unless the specific offence provides otherwise. These provisions set out default rules regarding pecuniary penalty to imprisonment ratios;[170] penalties for corporations;[171] and different penalties for summary and indictable proceedings.[172]

9.140 The ALRC has identified a number of specific secrecy offences which are inconsistent with the approach set out under the *Crimes Act*, including 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*;[173]

- the maximum fines applicable to bodies corporate provided under some secrecy offences differ from the 'times five' multiplier provided by s 4B(3) of the *Crimes Act*;[174]

---

168 Ibid.

169 Ibid.

170 *Crimes Act 1914* (Cth) s 4B(2) provides that where an offence provision refers only to a penalty of imprisonment, a court may impose a pecuniary penalty if it thinks it appropriate. The maximum pecuniary penalty is five times the term of imprisonment expressed in months.

171 Ibid s 4B(3) provides that where a body corporate is convicted of an offence, the court may impose a pecuniary penalty not exceeding an amount equal to five times the maximum penalty that the court could impose on a natural person convicted of the same offence.

172 Ibid ss 4J, 4JA.

173 For example, the ratio provided by the *Excise Act 1901* (Cth) s 159 is more than 20:1 (500 penalty units and two 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 one year of 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, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 41.

174 See, eg, *Defence Act 1903* (Cth) s 73F(2) which 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*;[175] and

- some secrecy provisions provide that they are summary offences, but include penalties which, under s 4H of the *Crimes Act*, would make the offence an indictable offence.[176]

9.141 In DP 74, the ALRC proposed that, in order to ensure consistency, specific secrecy offences should not stipulate:

- fines for individuals and corporations different from those that would apply if the formulas set out in the *Crimes Act* were adopted;

- penalties different from those that would apply if the alternative penalties for proceeding summarily on an indictable offence set out in the *Crimes Act* were adopted; or

- 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.[177]

Penalty benchmarks

9.142 The *Guide to Framing Commonwealth Offences* sets out principles for setting penalties in Commonwealth criminal offences. As a general principle, the *Guide* states that:

> A maximum penalty should be adequate and appropriate to act as an effective deterrent to commission of the offence to which it applies, and should reflect the seriousness of the offence in the relevant legislative scheme. A heavier penalty will be appropriate where there are strong incentives to commit the offence, or where the consequences of the commission of the offence are particularly dangerous or damaging.[178]

9.143 The *Guide* also sets out penalty benchmarks for certain classes of offences.[179] It specifies a maximum penalty benchmark of two years imprisonment or 120 penalty units for breach of secrecy provisions—citing as examples provisions which relate to

---

175 See, eg, *Disability Services Act 1986* (Cth) s 28 and *Telecommunications (Interception and Access) Act 1979* (Cth) s 105 which 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.

176 See, eg, *Taxation (Interest on Overpayments and Early Payments) Act 1983* (Cth) s 8 which provides for a maximum penalty of two years imprisonment and an $11,000 fine, punishable on summary conviction.

177 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 11–4.

178 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 38.

179 Ibid, 47.

both initial[180] and subsequent[181] unauthorised disclosure of Commonwealth information.

9.144 The exercise of judicial discretion in sentencing allows the imposition of a lower penalty if justified by the nature and circumstances of the offence and any injury, loss or damage resulting from the offence.[182]

9.145 The *Guide* directs those framing offences to 'ensure [the] penalty fits with other penalties in Commonwealth law':

> 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.[183]

9.146 Therefore, the penalties for contravention of specific secrecy offences—which, in the ALRC's view, should generally include a requirement that the disclosure cause, or be likely or intended to cause harm to an essential public interest[184]—should be comparable to penalties for conduct that causes similar kinds of harm and consistent with the culpability of the offender, which will be determined by a number of factors including the fault elements that apply to the offence.

9.147 Other benchmarks specified in the *Guide to Framing Commonwealth Offences* are relevant in gauging the relative criminality of conduct that results in harm to public interests. For example, the *Guide* includes the following penalty 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;
- two years imprisonment, or 120 penalty units, for breaching confidentiality requirements and for making false statements in applications for warrants;
- five years imprisonment, or 300 penalty units, for corruption and abuse of public office; and

---

180 *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).

181 *Australian Hearing Services Act 1991* (Cth) s 67(8).

182 *Crimes Act 1914* (Cth) s 16A(2).

183 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 38.

184 Recommendations 8–1, 8–2.

- life imprisonment for treason, certain war crimes and terrorist acts.[185]

9.148 Other federal offences that result in harm to public interests may also provide a guide for developing penalties for the breach of secrecy offences. For example, it is an offence for any person to disclose information about the identity or location of a person in the National Witness Protection Program, or information which compromises the security of such a person.[186] Because of the serious harm that is likely to be caused by disclosure in breach of this provision, a maximum penalty of 10 years is prescribed.

9.149 In DP 74, the ALRC proposed that 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.[187] The ALRC also proposed that where an offence includes a requirement that the disclosure causes, or is likely or intended to cause, harm to an essential public interest, the penalty should be consistent with those proposed in the general secrecy offence. For example, where a person knows, is reckless as to whether, or intends the disclosure of Commonwealth information to damage, for example, national security the penalty should be a maximum of seven years imprisonment, or a pecuniary penalty not exceeding 420 penalty units, or both.[188]

9.150 Finally, the ALRC has identified seven secrecy offences that specify maximum terms of imprisonment of three months.[189] 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:

> 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.[190]

9.151 In DP 74, the ALRC proposed that 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.[191]

---

185 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 47–48.

186 *Witness Protection Act 1994* (Cth) s 22.

187 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 11–8.

188 Ibid, Proposals 11–9, 11–10.

189 *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.

190 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 42–43.

191 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 11–11.

Submissions and consultations

9.152 While only a few stakeholders commented on the proposals in DP 74 relating to penalties for specific secrecy offences, the common theme was support for consistency and the legal principle that similar offences should have similar penalties.

9.153 Liberty Victoria and CLA both supported a review of penalties to ensure consistency.[192] The ACC expressed support for the general principle that penalties for secrecy offences should be consistent, but noted that in some circumstances there may be legitimate reasons why some penalties are higher or lower than others. For example, the ACC submitted that some penalties in the *Australian Crime Commission Act* are high because of difficulties experienced in achieving compliance with coercive powers exercised by ACC examiners.[193]

9.154 In response to the discussion of appropriate penalties in IP 34,[194] 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.[195]

9.155 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.[196]

9.156 The Law Council of Australia submitted that maximum penalties for secrecy offences should be 'identified and set by reference to the kind of information protected'.[197] The Public Interest Advocacy Centre submitted that:

---

192 Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

193 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

194 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Questions 5–4, 5–6.

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

196 Ibid.

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

> 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.[198]

9.157 A number of stakeholders submitted that secrecy offences should provide penalties that are consistent with the general provisions of Part IA of the *Crimes Act.*[199]

ALRC's views

9.158 In this Report, the ALRC recommends that specific secrecy offences should be used only where they are necessary to protect an essential public interest of sufficient importance to justify criminal sanction.[200] Criminal penalties for disclosure of Commonwealth information should be reserved for disclosures that cause, or are likely or intended to cause, harm to essential public interests.[201]

9.159 The penalty stated in a specific secrecy offence will therefore depend on the nature of the harm arising from the unauthorised disclosure of the information and the fault elements that apply to the particular offence.

9.160 In some cases, a higher maximum penalty will be appropriate: for example, where the fault element attaching to the harm, or the seriousness of the harm caused, or likely to be caused, by the disclosure, indicate a higher level of culpability.

9.161 In relation to the general secrecy offence, the ALRC recommends that a maximum penalty of seven years imprisonment is appropriate where a Commonwealth officer knows, or is reckless as to whether, or intends the disclosure of Commonwealth information to cause harm to:

- national security, defence or the international relations of the Commonwealth;
- the prevention, detection, investigation, prosecution or punishment of criminal offences;
- the life or physical safety of any person; or
- the protection of public safety.[202]

---

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

199 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.

200 Recommendation 8–1.

201 Recommendation 8–2.

202 Recommendation 5–1.

9.162 The higher maximum penalty recommended in the general secrecy offence is intended to reflect the higher culpability of the offender—indicated by the fault element attaching to the harm and the seriousness of the harm that is likely to be caused.

9.163 As discussed in Chapter 8, there may be a need for specific secrecy offences to address harms not included in the general secrecy offence. For example, regulatory agencies, such as taxation and social security agencies and corporate regulators, need to strictly control sensitive personal and commercial information provided to them by the public. In these cases, the ALRC considers that the unauthorised disclosure of this information has the potential to harm the relationship of trust between the government and individuals, and compromise the effective functioning of these regulatory agencies—harms not included in the recommended general secrecy offence. In such cases, the ALRC considers that a maximum penalty of two years imprisonment, or 120 penalty units would reflect the nature of the harm arising from the disclosure and would be consistent with other similar offences.

9.164 In some cases, the ALRC's recommended approach will mean that specific secrecy offences include tiers of offences that attract different penalties. The secrecy offences in the *Surveillance Devices Act 2004* (Cth), which make it an offence to disclose protected information, take this approach. Protected information includes any information obtained from the use of a surveillance device, information relating to an application for, or existence of, a warrant, or any information that is likely to enable the identification of a person, object or premises specified in a warrant.[203] The offence of unauthorised use, recording or disclosure of protected information carries a maximum penalty of two years imprisonment[204]—which seems appropriate, given the need to protect information about, or obtained by covert surveillance.[205] However, where the same conduct 'endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence'—both serious harms commensurate with those in the general secrecy offence—the offence provides for a higher penalty of 10 years imprisonment.[206]

---

203 *Surveillance Devices Act 2004* (Cth) s 45. Protected information is defined in s 44.

204 Ibid s 45(1).

205 This offence does not include an express requirement that the disclosure cause, or is likely or intended to cause, harm to an essential public interest. However, like information obtained by a telecommunications interception, discussed in Ch 8, the category of information protected by this offence is precisely defined, and there are persuasive policy arguments for its absolute protection, including that covert surveillance involves a serious invasion of privacy. As such, it may not be appropriate for the offence to expressly require that the disclosure cause, or be likely or intended to cause, harm.

206 *Surveillance Devices Act 2004* (Cth) s 45(2). Because the *Surveillance Devices Act* is part of a national scheme, most states have enacted mirror offences with similar penalties: Attorney-General's Department, *Submission SR 67,* 14 August 2009.

9.165 In the ALRC's view, a particularly low penalty suggests that the specific secrecy offence is not directed to preventing disclosures that are likely to cause harm of sufficient seriousness to warrant a criminal offence. Given that there are a range of other mechanisms in place to protect government information—including administrative sanctions, contractual obligations and the general law—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.[207]

9.166 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* in relation to the fine to imprisonment ratio and penalties for summary and indictable offences. Such provisions should be reviewed with a view to bringing them into line with the criteria in the *Crimes Act.*

Recommendation 9–8 Maximum penalties in specific secrecy offences should reflect the seriousness of the potential harm caused by the unauthorised conduct and the fault elements that attach to the elements of the offence.

Recommendation 9–9 Specific secrecy offences should not generally prescribe:

(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 alternative 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 on indictment.

207 The review of specific secrecy offences is discussed in Ch 11.

10. Authorised Disclosure Provisions

Contents

Introduction

10.1 While the primary focus of secrecy offences is to prohibit the disclosure of information, many secrecy provisions also set out circumstances in which the disclosure of information is permitted. These are often framed as exceptions to an offence, but some legislation contains rules for the handling of information that stand alone and are not tied to an offence.

10.2 In Chapter 7, the ALRC discusses the exceptions which, in its view, should be included in the general secrecy offence. This chapter considers how authorised disclosure provisions in specific legislation can provide content to some of the recommended exceptions in the general secrecy offence.

10.3 Authorised disclosure provisions, whether framed as exceptions to a secrecy offence or as stand-alone information-handling rules, often reflect the need for the government to share information within and between governments, and in some instances, with the private sector. This chapter also considers when it may be appropriate to include exceptions in specific secrecy offences, and the form that those exceptions should take.[1]

Authorised disclosure provisions

10.4 In this chapter, the ALRC uses the term 'authorised disclosure provisions' to refer to three kinds of provision that operate to permit the disclosure of government information—exceptions; defences; and information-handling provisions.

Exceptions

10.5 Most secrecy provisions contain exceptions to the prohibition on disclosure. An 'exception' is a provision that limits the scope of the conduct prohibited by a secrecy offence (compared to a 'defence', which operates to excuse conduct that is prohibited by the offence). An exception may provide, for example, that a person does not commit an offence where the disclosure of information is made in the course of performing duties under the relevant legislation.

10.6 Examples of the range of exceptions that may be included in specific secrecy provisions are summarised in Chapter 3, and include disclosures that are:

- in the course of an officer's functions and duties;
- for the purposes of specific legislation;
- authorised by specified persons;
- made to specified persons or entities;
- for the purposes of legal proceedings or law enforcement;
- made with the consent of the person to whom the information relates;
- made to avert threats to life or health; or
- in the public interest.

---

1 The operation of particular information-sharing arrangements, such as memorandums of understanding, interagency guidelines and legislative information-handling regimes are discussed in Ch 14.

10.7 The most common exceptions in specific secrecy offences are those that permit disclosure in the performance of a person's functions and duties or for the purposes of particular legislation. Exceptions that fall into one or both of these categories are present in approximately two thirds of all secrecy offences. Approximately 20% of offences allow disclosure with the authority of a specified person, such as the head of an agency.

10.8 A common formulation is to place a general prohibition on the disclosure of certain information and then to codify circumstances in which disclosure is allowed. One example is the *Income Tax Assessment Act 1936* (Cth), which allows the Commissioner, a Second Commissioner, or a Deputy Commissioner of Taxation or a delegate to authorise disclosure to a wide range of specified bodies, set out in 30 separate subparagraphs.[2] Another example is the *Law Enforcement Integrity Commissioner Act 2006* (Cth), which contains exceptions to secrecy obligations placed on the staff members of the Australian Commission for Law Enforcement Integrity. The provisions allow the Integrity Commissioner to disclose information in prescribed circumstances, including to the heads of a range of specified Commonwealth, state and territory agencies.[3] Many other secrecy offences follow a similar approach.[4]

Defences

10.9 A defence excuses conduct that is prohibited by an offence. Although specific secrecy offences generally contain exceptions rather than defences, examples of defences in specific secrecy offences include:

- s 200A(3) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth)—which provides that 'it is a defence to a prosecution' for disclosing information if the information was communicated to a person authorised in writing by the person to whose affairs the document relates;[5]

- s 58(3) of the *Defence Force Discipline Act 1982* (Cth)—which provides a defence to a prosecution for the 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';

---

2 *Income Tax Assessment Act 1936* (Cth) s 16(4)(a)–(m). The Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) 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.

3 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 208(3).

4 See, eg, *Dental Benefits Act 2008* (Cth) ss 34–41; *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 122; *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30; *Aged Care Act 1997* (Cth) ss 86-2, 86-3.

5 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 191(2A) contains a similar defence.

- s 79(5) and (6) of the *Crimes Act 1914* (Cth)—which provide that a person who receives certain information, knowing or having reasonable ground to believe that it is communicated in contravention of particular secrecy offences, shall be guilty of an offence 'unless he or she proves that the communication was contrary to his or her desire'; and

- s 91.2 of the *Criminal Code* (Cth)—which provides a defence to the prosecution of an offence of communicating information if it is 'information that has already been communicated or made available to the public with the authority of the Commonwealth'.

10.10 Approximately 10% of secrecy offences do not contain express exceptions or defences. Defences may nevertheless be available under provisions of the *Criminal Code* or at common law. Chapter 7 summarises the defences of general application contained in pt 2.3 of the *Criminal Code,* in particular the defence of 'lawful authority', which applies where 'the conduct constituting the offence is justified or excused by or under a law'.[6]

Information-handling provisions

10.11 Some legislation that does not contain specific secrecy offences may set out circumstances in which certain information may be disclosed. The ALRC has not classified such provisions as 'secrecy provisions' because they do not prohibit the disclosure of information—rather, they establish rules about the handling and disclosure of information. However, such provisions may operate as exceptions to obligations of non-disclosure set out in other legislation.

10.12 For example, s 718 of the *Fair Work Act 2009* (Cth) permits the Fair Work Ombudsman to disclose information acquired by the Ombudsman, or persons working for or assisting the Ombudsman, where the disclosure is:

- necessary or appropriate in the course of exercising functions or powers under the Act;

- likely to assist in the administration or enforcement of a Commonwealth, state or territory law;

- to assist the Minister to consider a matter arising under the Act; or

- to the Department for the purposes of briefing the Minister.

---

6 *Criminal Code* (Cth) s 10.5.

10.13 The Explanatory Memorandum explains that this provision

> is intended to operate in conjunction with relevant provisions in the *Privacy Act 1988* and the *Public Service Act 1999* and *Public Service Regulations 1999* (including the APS Code of Conduct).[7]

10.14 So, for example, the disclosures authorised under s 718 of the *Fair Work Act* are indicative of the disclosures that fall within the exceptions to the prohibition of disclosure contained in reg 2.1 of the *Public Service Regulations* that binds all Australian Public Service employees.

Interaction with the exceptions in the general secrecy offence

10.15 In Chapter 7, the ALRC recommends that the general secrecy offence should include three 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.[8]

10.16 Because the recommended general secrecy offence will apply to current and former Commonwealth officers across all Commonwealth agencies, these exceptions are necessarily widely drawn. As discussed in Chapter 7, the ALRC considers that, while it would not be possible to include a comprehensive list of disclosures that fall within these exceptions in the general secrecy offence, clarity about the scope of the exceptions should be provided in other ways, for example, in legislation regulating specific agencies.

10.17 The following section considers how authorised disclosure provisions in specific legislation will interact with the recommended general secrecy offence. In particular, this section examines how authorised disclosure provisions will give substance to the exceptions in the general secrecy offence for disclosures 'in the course of an officer's functions or duties' and to the *Criminal Code* defence of lawful authority.

In the course of an officer's functions or duties

10.18 The ALRC recommends that the general secrecy offence include an exception for disclosures 'in the course of a Commonwealth officer's functions or duties'.[9] As

---

7 Explanatory Memorandum, Fair Work Bill 2008 (Cth), 404.
8 Recommendation 7–1.
9 Recommendation 7–1.

noted in Chapter 7, exceptions permitting disclosures in the performance of duties as an officer have been given a wide interpretation by the High Court, and encompass matters incidental to carrying out the functions and duties authorised by an officer's employment.[10]

10.19 However, the duties authorised by an officer's employment extend only to those duties that have some basis in legislation governing the officer, such as legislation administered by the specific agency or the *Public Service Act 1999* (Cth). This requirement can limit the operation of the exception in secrecy provisions, particularly where an officer seeks to disclose information for purposes that are not directly related to the core functions set out in the legislation governing his or her agency.

10.20 Legal advice from the Australian Government Solicitor (AGS), attached to the *Report of a Review of Information Handling Practices in the Serious Non Compliance Business Line of the Australian Taxation Office* (AGS advice),[11] provides an example of the limited scope of the 'performance of duties' exception in this regard. The AGS was asked whether officers of the Australian Taxation Office (ATO) could provide information under the *Mutual Assistance in Criminal Matters Act 1987* (Cth). Section 13A of that Act allows the Attorney-General to authorise the provision of material to a foreign country. However, because taxation laws do not expressly authorise officers to share information for the purposes of mutual assistance, and because the *Mutual Assistance in Criminal Matters Act* does not specifically give the ATO a role in the administration of the scheme, the AGS expressed the view that the disclosure of information for the purposes of the *Mutual Assistance in Criminal Matters Act* did not fall within the performance of an ATO officer's duties.[12]

10.21 The AGS also advised that duties imposed by Commonwealth policies and guidelines, or under international agreements, could not provide a basis for the 'performance of duties' exception, unless such policies or agreements were supported by statute.[13]

10.22 Therefore, an officer's duties and functions cannot be determined in a vacuum—they must be grounded in legislation, particularly where those duties and functions may operate as an exception to a criminal offence. To this end, in Chapter 7 the ALRC expresses the view that the legislation regulating specific agencies, or more general instruments such as the *Public Service Act*, will be indicative of what falls within an officer's duties or functions.

---

10 *Canadian Pacific Tobacco Co Ltd v Stapleton* (1952) 86 CLR 1, 6.

11 D Boucher, *Report of a Review of Information Handling Practices in the Serious Non Compliance Business Line of the Australian Taxation Office* (2008), Attachment 9.

12 Ibid, Attachment 9, 23–24.

13 Ibid, Attachment 9, 22–25. See, eg, *International Tax Agreements Act 1953* (Cth) s 23 which provides that disclosing information in accordance with the Commissioner's obligations under an international agreement is not a breach of a secrecy provision in a taxation law.

Lawful authority

10.23 As discussed in Chapter 7, the *Criminal Code* contains a defence of 'lawful authority' where 'the conduct constituting the offence is justified or excused by or under a law'.[14] The ALRC has not, therefore, recommended that the general secrecy offence expressly include an exception for disclosures that are 'authorised or required by law'.

10.24 The application of this defence to the recommended general secrecy offence would mean that the existence of a 'law of the Commonwealth' that authorises a disclosure would operate as an exception to the prohibition on disclosure in the general secrecy offence.[15] As with the 'performance of duties' exception, where such disclosures are made pursuant to a policy or executive guideline, such policies and guidelines would need to be consistent with any underlying legislation.

Submissions and consultations

10.25 In response to the Discussion Paper, *Review of Secrecy Laws* (DP 74), a number of stakeholders commented on the interaction between the general secrecy offence and specific secrecy provisions.

10.26 Some agencies were concerned that the exceptions in the general secrecy offence were wider or more flexible than exceptions in current specific secrecy provisions. The Department of Health and Ageing (DoHA) noted, for example, that the general secrecy offence would allow an agency head or minister to authorise the disclosure of information where it is in the public interest. However, s 130(3)(a) of the *Health Insurance Act 1973* (Cth)

> currently permits the release of confidential Medicare information where the Minister certifies, by instrument in writing, that release is 'necessary in the public interest'. Any proposal to remove the word 'necessary' from the legislation, or to otherwise dilute it, would almost certainly be opposed by consumers and medical organisations.[16]

10.27 In addition, DoHA expressed concern that the proposed general secrecy offence would not capture exceptions unique to particular secrecy provisions, such as exceptions that allow the release of personal information with the informed consent of the person to whom the information relates.[17]

---

14 *Criminal Code* (Cth) s 10.5.

15 Australian Government Attorney-General's Department and the Australian Institute of Judicial Administration, *The Commonwealth Criminal Code: A Guide for Practitioners* (2002), 233.

16 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.

17 Ibid.

10.28 The Australian Transaction Reports and Analysis Centre (AUSTRAC) drew attention to the need for specific secrecy provisions to support and give content to exceptions in the general secrecy offence:

> The exception 'in the course of a Commonwealth officer's functions or duties' in the general secrecy offence needs to be underpinned by specific secrecy provisions that define the ambit of those functions and duties. AUSTRAC believes that the duties and functions of a Commonwealth officer of a statutory agency should be defined in accordance with the respective pieces of legislation that govern the operation of that agency.[18]

10.29 AUSTRAC submitted that it would not be appropriate for agency guidelines or memorandums of understanding (MOUs) to specify the disclosures that fall within an officer's functions or duties:

> The proposal to narrow the scope of the term by issuing agency guidelines or inter-agency memorandums of understanding is problematic as they would not be legally binding and would need to be job specific ...
>
> AUSTRAC believes that MOUs are important in establishing the expectations of the parties in respect to the exchange of information. However, AUSTRAC notes that in the majority of cases, MOUs are underpinned by specific secrecy provisions that regulate the disclosure of information, such as s 128 of the [*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)] and s 127 of the *Australian Securities and Investments Commission Act 2001* (Cth). These secrecy provisions provide certainty to the parties as to when and in what circumstances information will be disclosed.[19]

ALRC's views

10.30 The exceptions and defences that will apply to the recommended general secrecy offence anticipate that specific legislation—for example, legislation governing particular agencies or government functions—will set out the duties and functions of officers, and, where necessary, the disclosures they are authorised to make.

10.31 So, for example, a person prosecuted under the general secrecy offence could rely on the 'lawful authority' defence where an authorised disclosure provision in specific legislation permitted the disclosure. Similarly, a person seeking to rely on the exception in the general secrecy offence for disclosures 'in the course of an officer's functions or duties' could use specific legislation to give content to those functions and duties.

10.32 A number of stakeholders expressed concerns that the exceptions in the recommended general secrecy offence would be wider than those in current specific secrecy offences, or that unique exceptions currently in specific secrecy offences were not reflected in the general secrecy offence. Authorised disclosure provisions which include specific exceptions that are not covered by the general secrecy offence—such

---

18 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.
19 Ibid.

as exceptions relating to the disclosure of information with the consent of the person to whom, or entity to which, the information relates, or disclosures to law enforcement agencies or other specified persons or entities—will act to define the limits of an officer's duties in a particular case. Where a specific provision allows an officer, for example, to disclose information with consent, any such disclosure will fall within the exception in the general secrecy offence for disclosure in the course of that officer's duties and functions. Where a specific provision does not allow disclosure with consent, the general offence will not operate to allow this.

10.33 In Chapter 11, the ALRC recommends that specific secrecy offences should be reviewed in accordance with the principles recommended in Chapters 8 to 10 of this Report, including the recommendation that specific secrecy offences are only warranted where they are necessary to protect an essential public interest of sufficient importance to justify criminal sanction. The ALRC recommends that, when reviewing specific secrecy offences, consideration should be given to whether any exceptions or authorised disclosure provisions should be retained in order to provide a legislative basis for information-sharing arrangements and to give content to the exceptions in the recommended general secrecy offence. Authorised disclosures need not be exceptions to a specific secrecy offence, but could stand alone as information-handling provisions decoupled from the offence provision.

Recommendation 10–1 Where a specific secrecy offence is repealed or amended as a result of Recommendation 11–1, consideration should be given as to whether any provisions which codify authorised information handling should be retained.

Exceptions in specific secrecy offences

10.34 The remainder of this chapter considers the operation of exceptions and defences in specific secrecy offences. Because specific secrecy offences apply to different kinds of information and address the information-sharing requirements of different agencies, exceptions vary considerably—and for legitimate reasons. This is not an area in which firm criteria can always be established, or where it is useful to have a generally applicable model exception provision.

10.35 This section discusses some issues identified by stakeholders regarding the operation of exceptions to specific secrecy offences and then examines particular exceptions to secrecy offences in order to develop, where appropriate, general principles.

The operation of exceptions

10.36 The Terms of Reference for this Inquiry require the ALRC to have regard to the increased need to share Commonwealth information within and between governments and with the private sector. In this Report, the ALRC concludes that a general secrecy offence and specific secrecy offences are necessary to protect essential public interests that may be harmed by the unauthorised disclosure of Commonwealth information. In this context, where all Commonwealth officers are subject to secrecy offences—the general secrecy offence, and perhaps also specific secrecy offences—authorised disclosure provisions are often the mechanisms that permit officers to share information, in appropriate circumstances. In addition, authorised disclosure provisions provide guidance and certainty to officers subject to an offence for mishandling information.

10.37 There is, however, a tension inherent in using a prohibition on the disclosure of information to authorise the disclosure of that information in some circumstances. The tension between protecting and sharing information and its effect on the terms of secrecy provisions was noted by Dixon J in the 1974 case of *Jackson v Magrath* regarding taxation secrecy provisions:

> There is plenty of evidence in the rather lengthy provisions ... that the conflict between the requirements of secrecy and the pull which the exigencies of administration inevitably exerted towards the free exchange of information among fiscal and other governmental departments has proved a recurring problem for the draftsman.[20]

Submissions and consultations

10.38 In the Issues Paper, *Review of Secrecy Laws* (IP 34), the ALRC asked whether federal secrecy provisions unduly inhibited the sharing of information between government agencies, and with the private sector.[21] Stakeholders drew attention to a number of issues in relation to the operation of exceptions to secrecy provisions, including the narrow scope of some exceptions and inconsistencies between exceptions.

10.39 A number of stakeholders noted the increasing need to share information in order to deliver government programs and implement policies but expressed concerns that the exceptions in secrecy provisions were unable to accommodate appropriate information sharing. The Australian Government Attorney-General's Department (AGD) noted that:

> 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

---

20 *Jackson v Magrath* (1947) 75 CLR 293, 312, cited in J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49 at 63.

21 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 1–2.

> may not reflect the actual need to share information across agencies with common responsibilities. Few agency operations are neatly contained within these artificial boundaries.[22]

10.40 The Department of Education, Employment and Workplace Relations gave an example of how agency-specific secrecy provisions can pose a barrier to service delivery:

> 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.[23]

10.41 The Department of Human Services (DHS) raised similar concerns about the operation of secrecy provisions in the course of the delivery of government services. The DHS noted that secrecy provisions 'impose a level of bureaucratic complexity in service delivery which is often seen by customers as "red tape" or simply poor performance on the part of the agency'. The DHS also commented that, for example, secrecy provisions inhibited Centrelink from sharing child protection information with states and territories, and prevented the DHS using its database to assist other government agencies to investigate or enforce the criminal law.[24]

10.42 The Community and Disability Services Ministers' Advisory Council (CDSMAC) also highlighted the importance of information sharing in the child protection context, and noted that secrecy provisions binding officers in Australian Government agencies—such as Centrelink, Medicare and the Family Court—hindered those agencies sharing information with state and territory child protection agencies.[25]

10.43 While some Australian Government agencies commented that the secrecy provisions governing their agencies provided an appropriate balance between protecting and sharing information,[26] other stakeholders emphasised the importance of secrecy provisions in restricting the sharing of information. The Australian Bureau of Statistics, while identifying the importance of being able to gain access to certain information from other agencies, highlighted the importance of tightly controlling

---

22 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
23 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.
24 Department of Human Services, *Submission SR 83,* 8 September 2009.
25 Community and Disability Services Ministers' Advisory Council, *Submission SR 80,* 28 August 2009.
26 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009; Australian Intelligence Community, *Submission SR 37,* 6 March 2009; Australian Federal Police, *Submission SR 33,* 3 March 2009; Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.

access to the information that it holds.[27] The Non-Custodial Parents Party expressed concerns that personal information held by the Australian Government was disclosed to a wide range of people and organisations through 'loopholes' in secrecy provisions.[28]

10.44 A number of stakeholders identified problems in the way that exceptions to secrecy provisions are drafted and interpreted. For example, the DHS commented on the tension between flexibility and accountability in relation to exceptions in secrecy provisions:

> 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.[29]

10.45 In a submission in response to IP 34, Ron Fraser observed that lengthy lists of exceptions, while often designed to facilitate the disclosure of information to other public authorities,[30] 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.[31]

10.46 In light of this, a number of stakeholders commented on the challenge of drafting a secrecy provision that balances the need to share information with the need to protect it.[32] Some stakeholders also noted that exceptions are often added to secrecy provisions in an ad hoc manner as issues in information sharing arise, leading to inconsistent drafting and interpretation.[33]

---

27 Australian Bureau of Statistics, *Submission SR 28,* 24 March 2009.
28 Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009.
29 Department of Human Services, *Submission SR 26,* 20 February 2009.
30 See, eg, *Health Insurance Act 1973* (Cth) s 130.
31 R Fraser, *Submission SR 42,* 23 March 2009.
32 Department of Climate Change, *Submission SR 27,* 23 February 2009; Department of Human Services, *Submission SR 26,* 20 February 2009; Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.
33 Australian Crime Commission, *Submission SR 75,* 19 August 2009; The Treasury, *Submission SR 22,* 19 February 2009.

ALRC's views

10.47 Exceptions to secrecy offences are necessary to facilitate the disclosure of information in appropriate circumstances. However, as illustrated by some of the submissions set out above, it is sometimes difficult to find the appropriate balance between the need to protect information and the need to share it. In particular, the need to share information can be frustrated by overly narrow agency-specific exceptions to secrecy offences. As noted in Chapter 2, there is an increasing need to share Commonwealth information between government agencies and externally in order to fulfil whole of government and multi-agency approaches to government service delivery.

10.48 While it is important to ensure that authorised disclosure provisions are not unduly restrictive, the content and form of authorised disclosure provisions must be guided by government policy in the context in which they operate. Therefore, while the following consideration of authorised disclosure provisions takes account of the increased emphasis on information sharing, the ALRC recognises that the policies behind each specific secrecy offence will differ, necessitating different approaches to authorised disclosure provisions in particular contexts.

In the performance of duties or for the purposes of an Act

10.49 Approximately 65% of secrecy provisions contain an exception to permit the disclosure of information in the performance of a person's functions and duties or for the purposes of particular legislation. These exceptions are phrased in various ways.

10.50 Some specific secrecy offences include exceptions for the disclosure of information in the performance of official duties: for example, for disclosures made 'in the performance of the person's duties as an officer',[34] 'in the course of the employee's duties',[35] 'official duty'[36] or 'official employment'.[37]

10.51 Other exceptions are tied to particular legislation: for example exceptions that allow the disclosure of information 'for the purposes of this Act',[38] for the purposes of other legislation,[39] or in the performance of duties under particular legislation.[40]

---

34 See, eg, *Higher Education Funding Act 1988* (Cth) s 78(4A); *Student Assistance Act 1973* (Cth) s 12ZU; *Income Tax Assessment Act 1936* (Cth) s 16(2A).

35 See, eg, *Public Service Regulations 1999* (Cth) reg 2.1(5)(a).

36 See, eg, *Defence Act 1903* (Cth) s 73A.

37 See, eg, *National Blood Authority Act 2003* (Cth) s 11 (1)(c).

38 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).

39 See, eg, *Australian Human Rights Commission Act 1986* (Cth) s 49(3); *Reserve Bank Act 1959* (Cth) s 79A(2).

40 See, eg, *Dental Benefits Act 2008* (Cth) s 35; *Pooled Development Funds Act 1992* (Cth) s 71; *Australian Hearing Services Act 1991* (Cth) s 67.

A number of secrecy provisions prohibit an official from disclosing protected information except when required or permitted by 'this Act or any other law of the Commonwealth; or a prescribed law of a State or internal Territory'.[41]

10.52 As noted above, an exception for 'disclosures in the performance of duties as an officer' has been interpreted widely to govern all that is incidental to carrying out the functions and duties authorised by an officer's employment. Case law suggests that this may include disclosures:

- in the performance of a duty arising under the common law;[42]
- where an officer is required to disclose information to a court[43] or a body with legal authority to compulsorily obtain information;[44]
- for the purposes of a criminal prosecution, where the proceedings relate to the general functions and duties of an officer under legislation;[45] and
- under the *Freedom of Information Act 1982* (Cth) (FOI Act) and other routine disclosures.[46]

10.53 However, where an exception is limited to disclosures for the purposes of, or in the performance of duties under, a particular Act, the exception is more limited. Such exceptions are unlikely to permit the disclosure of information for the purposes of other legislation, or for purposes that are not directly related to the core functions set out in the legislation governing that agency. In particular, where 'performance of duties' or 'for the purposes of' exceptions are linked to particular legislation, the exception is unlikely to permit disclosures for purposes related to other legislation, including disclosures under the FOI Act or to integrity agencies.[47]

---

41 See, eg, *Offshore Petroleum and Greenhouse Gas Storage Act 2006* (Cth) s 758; *Australian Securities and Investments Commission Act 2001* (Cth) s 127(2); *Trade Practices Act 1974* (Cth) s 155AAA.

42 *Australian Institute of Marine and Power Engineers v Secretary, Department of Transport* (1986) 13 FCR 124; D Boucher, *Report of a Review of Information Handling Practices in the Serious Non Compliance Business Line of the Australian Taxation Office* (2008), Attachment 9, 17.

43 *Commonwealth v Fernie* (1999) 23 SR (WA) 12. In taxation legislation, the disclosure of information to courts is limited by s 16(3) of the *Income Tax Assessment Act 1936* (Cth) which permits disclosures to a court where necessary for the purpose of carrying into effect the provisions of the *Income Tax Assessment Act 1936* (Cth) or other taxation law. Courts have held such disclosures may be in the performance of duties where the proceedings relate to the imposition, assessment or collection of revenue: *Commissioner of Taxation v Nestle Australia Ltd* (1986) 12 FCR 257, 262–263.

44 *Mobil Oil Australia Pty Ltd v Commissioner of Taxation* (1963) 113 CLR 475, 505.

45 *R v Yates* (1991) 102 ALR 673.

46 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [9.1.4], citing *Canadian Pacific Tobacco Co Ltd v Stapleton* (1952) 86 CLR 1. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.98].

47 The interaction between secrecy laws and the *Freedom of Information Act 1982* (Cth) is discussed in Ch 16. The provision of information to integrity agencies is discussed later in this chapter.

10.54 A number of secrecy provisions deal with this issue by including detailed exceptions to permit information to be disclosed for the purposes of other legislation or intergovernmental arrangements.[48]

Submissions and consultations

10.55 In DP 74, the ALRC did not make any proposals in relation to exceptions in specific secrecy offences for disclosures in the performance of an officer's duties or for the purposes of particular legislation. However, in commenting on the proposed exception to the general secrecy offence for disclosures 'in the course of a Commonwealth officer's functions and duties',[49] the ATO noted that the 'performance of duties exception' is essential to the proper administration of the taxation laws:

> it is not possible to codify every circumstance in which a disclosure of taxpayer information should be permitted. As such, the performance of duties exception is flexible enough to allow a range of disclosures which are made in connection with the ATO's administration of the taxation laws.[50]

10.56 In response to IP 34, the DHS submitted that the formulation of this exception was inconsistent across the secrecy provisions within their portfolio, and that consistency of terminology would aid in the understanding of the provisions:

> 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* [*1988* (Cth)] s 16);
> - 'in the performance of duties, or in the exercise of powers or functions under this Act' (*National Health Act* [*1953* (Cth)] s 135A); and
> - 'authorised by or under the social security law' (ss 203 and 204 *Social Security (Administration) Act* [*1999* (Cth)]).
>
> 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'.[51]

ALRC's views

10.57 The increasing need to share Commonwealth information within and between governments and with the private sector was identified in the Terms of Reference for

---

48 For example, the *Racial Discrimination Act 1975* (Cth) s 27F(3)(b) permits the disclosure of information pursuant to intergovernmental arrangements permitted under s 16 of the *Australian Human Rights Commission Act 1986* (Cth). Similar provisions are included in the *Age Discrimination Act 2004* (Cth) s 60(3); *Disability Discrimination Act 1992* (Cth) s 127(3); *Sex Discrimination Act 1984* (Cth) s 112(3).

49 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–1.

50 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

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

this Inquiry,[52] and is evident in the trend towards coordinated, whole of government policy development and implementation.[53] In the ALRC's view, an exception to permit the disclosure of information in the performance of an officer's duties is critical for information sharing in these contexts.

10.58 If there is a policy intention to permit information protected by a secrecy offence to be shared with other government agencies or entities beyond government, a performance of duties exception should be broadly framed so as to permit disclosures in the performance of a person's functions and duties as an officer. This will permit a greater degree of sharing than an exception limited to disclosures in the performance of duties under particular legislation, or for the purposes of a particular Act. A broadly framed 'performance of duties as an officer' exception will also ensure that disclosures for purposes related to other legislation, including disclosures under the FOI Act or to integrity agencies, are not precluded.

10.59 A performance of duties exception will be limited by the legislative framework that governs an officer and, therefore, will not always support the needs of agencies to share information in particular circumstances. Where information needs to be shared for the purposes of unrelated legislation, it will be necessary for legislation to specify this in a more detailed list of permitted disclosures. Alternatively, a provision could permit the disclosure of information for the purposes of legislation to be prescribed in regulations. It may be that other provisions, such as the objects of the Act, should also reflect information-sharing policies.

10.60 Finally, while it is important to ensure that authorised disclosure provisions reflect government policy and are not unduly restrictive, some specific secrecy offences may require narrowly framed exceptions to reflect the policy that the information protected by the secrecy offence should only be disclosed in limited circumstances.

Recommendation 10–2 Specific secrecy provisions that impose secrecy obligations on officers should generally include an exception for disclosures in the course of an officer's functions or duties.

Authorised by specified persons

10.61 A number of secrecy provisions permit the disclosure of information at the discretion of specified office-holders or other persons.

52 The Terms of Reference are set out at the front of this Report.
53 This is discussed in Ch 2.

10.62 Some provisions include an exception to allow any person to disclose information where that disclosure is authorised by an agency head for a particular purpose. For example, the *Customs Administration Act 1985* (Cth) includes an exception 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.[54] Other exceptions rely solely on the discretion of the agency head. For example, an officer of the Australian Security Intelligence Organisation does not commit an offence if disclosing information 'with the approval of the Director-General' or his or her delegate.[55]

10.63 Other exceptions set out a scheme whereby a minister or senior official (usually a departmental secretary or agency head) can certify that it is in the public interest to disclose particular information. For example, the secrecy offence in the *A New Tax System (Family Assistance) (Administration) Act 1999* (Cth) provides an exception where the Secretary certifies that it is necessary in the public interest to disclose protected information to such persons and for such purposes as the Secretary determines.[56] In issuing a public interest certificate under this section, the Secretary must act in accordance with guidelines set by the Minister.[57] The current guidelines specify a number of matters to which the Secretary must have regard and envisage the issuing of public interest certificates for a range of purposes, including:

- to prevent, or lessen, a threat to the life, health or welfare of a person;
- for the enforcement of a criminal law, imposition of pecuniary penalty or prevention of an act that may have a significant adverse effect on the public revenue;
- to assist a court or other authorities to ascertain the whereabouts of a missing person, or to locate a person or a relative or beneficiary of a deceased person;
- to brief a minister; or
- for research and statistical analysis or policy development.[58]

---

54 *Customs Administration Act 1985* (Cth) s 16(3). See also *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 129(1); *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C(5)(b).

55 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(2)(c).

56 *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 168.

57 Ibid s 168(3).

58 *A New Tax System (Family Assistance) (Administration) (Public Interest Certificate Guidelines) (DEEWR) Determination 2009 (No 1)* (Cth). This model is replicated in *Social Security (Administration) Act 1999* (Cth) ss 208–209; *Student Assistance Act 1973* (Cth) s 356(1)(a); *Child Care Act 1972* (Cth) ss 12N, 12P.

10.64 Some other exceptions require a minister to issue a public interest certificate in order to permit a departmental secretary or agency head to disclose protected information.[59]

10.65 Finally, some exceptions permit an agency head to disclose information in certain circumstances where it is in the public interest, without the need to issue a certificate.[60] These exceptions vary as to the considerations that an agency head must take into account when determining what is in the public interest. Some provisions of this kind also detail procedural fairness obligations in relation to the disclosure of information in the public interest.[61]

10.66 The effect of such provisions is that, where the agency head or other senior official has validly exercised his or her discretion, a person who discloses information with such authority will not be liable under a secrecy offence.

10.67 Concerns have been expressed, however, that an exception that allows the disclosure of information with the authority of an agency head or senior official is an inappropriate delegation of power, on the basis that it effectively enables him or her to determine the scope of an offence without parliamentary scrutiny. For example, commenting on a provision that created an offence of failing to comply with a security direction issued by an agency head, the Senate Standing Committee for the Scrutiny of Bills (Scrutiny of Bills Committee) stated that:

> The discretionary nature of this provision overturns a fundamental principle by which penalties for criminal conduct are imposed. A person should not be exposed to a penalty or criminal sanction at the discretion of an official. The decision as to what is criminal conduct is more preferably left to the Parliament.[62]

Submissions and consultations

10.68 In DP 74, the ALRC proposed that the general secrecy offence contain an exception applying where the disclosure is 'authorised by the relevant agency head or minister, and the agency head or minister certifies that the disclosure is in the public interest'.[63] While the ALRC did not make any proposals on this issue in relation to specific secrecy offences, some submissions were instructive in this regard.

---

59 See, eg, *Health Insurance Act 1973* (Cth) s 130(3); *National Health Act 1953* (Cth) s 135A(3).

60 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 209; *Ombudsman Act 1976* (Cth) s 35A.

61 See, eg, *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 210.

62 Parliament of Australia—Senate Standing Committee for the Scrutiny of Bills, *Fourteenth Report of 2003* (2003), 309–311.

63 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 9–1.

10.69 The ATO and the Treasury did not support an exception in either the general or specific secrecy offences to allow an agency head to authorise disclosures on a case-by-case basis.[64] The ATO submitted that:

> It is conceivable that a minister or agency head could authorise the disclosure of taxpayer information for purposes which could broadly be considered to be in the public interest, but which may damage the reputation of the individual or corporation whose information is being released. Further the ATO considers that the discretionary nature of such an exemption would reduce certainty for taxpayers and could impact upon compliance with their taxation obligations.[65]

10.70 The Treasury considered that the authorisation of disclosures in the public interest was a matter to be considered by the Parliament, not members of the executive:

> This provides both the holders of information (for instance, taxation officers) and the sources of the information (notably, the Australian public) both certainty as to when information can be lawfully disclosed (including authorised disclosures in instruments of authorisation arguably limits the transparency of such disclosures) and the confidence that disclosures will be made only in appropriate circumstances.[66]

10.71 The Australian Privacy Foundation commented that an unlimited ad hoc ability to authorise exceptions was objectionable and should be subject to objective public interest criteria, adequate controls and reporting requirements to prevent abuse.[67]

10.72 In contrast, in response to IP 34, the AGD considered that a provision to enable an agency head or other senior officers to authorise disclosure might

> 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.[68]

ALRC's views

10.73 Exceptions that allow the disclosure of protected information in the public interest accord with principles of open and accountable government. In addition, as discussed in Chapter 8, consistency with Australia's international human rights obligations, it is important that secrecy provisions do not impose an unjustified and excessive burden on the right to freedom of expression.[69] In *R v Shayler,* the House of Lords suggested that a secrecy offence may be a necessary and proportionate

---

64 The Treasury, *Submission SR 60,* 10 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

65 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

66 The Treasury, *Submission SR 60,* 10 August 2009.

67 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

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

69 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976) art 19.

restriction on freedom of expression if it does not constitute an absolute ban on disclosures, and includes avenues for officers to make authorised disclosures, such as under a public interest disclosure regime or procedures for seeking authorisation for making particular disclosures.[70]

10.74 Exceptions that permit disclosures with the authorisation of a senior official or minister are sometimes necessary, particularly where a level of flexibility is needed in order to respond to emergencies or unexpected circumstances. An exception of this kind would allow a person to seek authorisation for the disclosure from a senior official who, due to their position, can make an informed judgment about the likely consequences of the disclosure, including balancing the public interests.

10.75 The ALRC notes the principles in relation to the delegation of legislative power stated by the Scrutiny of Bills Committee, in particular the principle that a person should not be subject to a criminal offence at the discretion of an official. The exception does not permit an agency head or minister to create a criminal offence, but rather protects an officer from prosecution where he or she has a valid authorisation to disclose the information. Further, in exercising discretion to authorise the disclosure of information, an agency head or minister is constrained by the principles of administrative law—including that any decision must be reasonable and made in good faith. The agency head or minister would have to be acting consistently with his or her governing legislative framework.

10.76 In Chapter 7, the ALRC recommends that the general secrecy offence include an exception where the disclosure is made in accordance with an authorisation given by an agency head or minister that the disclosure would, on balance, be in the public interest.[71] As discussed in Chapter 7, the subject matter and purpose of the legislation—that is, the *Criminal Code*—will be relevant in construing the scope of this exception, including the public interests protected by the general secrecy offence.

10.77 There are a number of other ways to guide the exercise of such a discretion in specific secrecy offences. Exceptions may set out the criteria by which an agency head or minister makes a decision to authorise the disclosure of information. Alternatively, guidelines issued by a minister could inform the exercise of a power to authorise disclosures in the public interest.

Information in the public domain

10.78 Some specific secrecy offences provide exceptions where the information disclosed is already in the public domain[72] or has lawfully been made available to the

70 *R v Shayler* [2003] 1 AC 247, 271, 284. This case is noted in Ch 2 and discussed in detail in Ch 8.
71 Recommendation 7–1.
72 See, eg, *Criminal Code* (Cth) s 91.2; *Offshore Minerals Act 1994* (Cth) s 375.

public.[73] Taxation secrecy laws, in contrast, can operate to prevent the ATO from disclosing publicly available information, such as the fact that a barrister has been convicted of a taxation offence.[74]

10.79 A distinction may be made between information that is in the public domain as the result of a lawful disclosure and as a result of an unlawful disclosure. Specific secrecy offences generally require that, for the exception to apply, the information was in the public domain because of a lawful disclosure. This ensures that a person who discloses information without authority cannot rely on an earlier unauthorised disclosure to justify his or her later, but still unauthorised, disclosure of the information.

Submissions and consultations

10.80 While the ALRC did not make any proposals on this matter in DP 74, some submissions in response to IP 34 considered an exception for the disclosure of information already in the public domain.

10.81 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.[75] This view is consistent with the Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) (Tax Laws Exposure Draft Bill), which provides that a taxation officer who discloses protected information does not commit an offence if the information was 'already lawfully available to the public'.[76]

10.82 Other stakeholders also supported the application of exceptions relating to the disclosure of information that is in the public domain.[77] The Commonwealth Director of Public Prosecutions, for example, stated that 'if investigation agencies are unable to publicise the outcomes of prosecutions the deterrent effect of successful prosecutions will be undermined'.[78]

---

73 See, eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(1) definitions of 'protected document' and 'protected information'.

74 New South Wales Bar Association, *Submission to Treasury Review of Taxation Secrecy and Disclosure Provisions*, 26 September 2006.

75 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

76 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cll 355-20–355-40.

77 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.

78 Commonwealth Director of Public Prosecutions, *Submission SR 17,* 18 February 2009.

ALRC's views

10.83 The ALRC considers that specific secrecy offences should not criminalise the disclosure of information that is lawfully in the public domain. In Chapter 7, the ALRC recommends that the general secrecy offence and the subsequent disclosure offences include an exception where the disclosure is of information that is already in the public domain as the result of a lawful disclosure.[79] Specific secrecy offences should generally also include such an exception, or define the information protected in such a way as to ensure that it does not cover publicly available information.

Recommendation 10–3 Specific secrecy offences should not apply to the disclosure of information that is lawfully in the public domain.

For the purposes of law enforcement

10.84 A number of specific secrecy provisions include exceptions to allow the disclosure of information for the purposes of law enforcement.[80] For example, s 38(1) of the *Dental Benefits Act 2008* (Cth) provides an exception to the prohibition on the disclosure of protected information where:

> (a) the Secretary or the Medicare Australia CEO believes on reasonable grounds that the disclosure is reasonably necessary for:
>
> (i) the enforcement of the criminal law; or
>
> (ii) the enforcement of a law imposing a pecuniary penalty; or
>
> (iii) the protection of the public revenue; and
>
> (b) the functions of the agency include that enforcement or protection; and
>
> (c) the disclosure is for the purposes of that enforcement or protection.

10.85 In Chapter 7, the ALRC sets out a number of submissions from government agencies that commented on the importance of ensuring that secrecy provisions did not prevent the disclosure of information to law enforcement or regulatory agencies. In that chapter, the ALRC recognises that the exchange of information with law enforcement and regulatory agencies is important in identifying, investigating and prosecuting unlawful activity, it may not be appropriate in all circumstances. For these reasons, the ALRC is not recommending that the general secrecy offence include a general exception for the disclosure of information for the purposes of law enforcement.

10.86 Such an exception may, however, be appropriate in specific secrecy provisions. As noted above, disclosures for the purposes of a criminal prosecution, where the proceedings relate to the general functions and duties of the officer under legislation,

---

79 Recommendations 7–1, 7–2.

80 See, eg, *Australian Citizenship Act 2007* (Cth) s 43(2)(ea); *Inspector of Transport Security Act 2006* (Cth) s 68; *Child Support (Assessment) Act 1989* (Cth) s 150(4D)–(4F).

will generally fall within a 'performance of functions and duties' exception. Alternatively, where it is appropriate to allow the disclosure of information for the purposes of law enforcement, an exception or information-handling provision could be included in agency-specific legislation.

For the purposes of legal proceedings

10.87 Some exceptions in specific secrecy offences permit the disclosure of information for the purposes of court or tribunal proceedings.[81]

10.88 In comparison, a number of specific secrecy offences provide that a person is not required to disclose information in court or tribunal processes, other than for particular purposes.[82] 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.

10.89 Similar conclusions can be made about exceptions to disclose information for the purposes of legal proceedings as for exceptions for disclosures for the purposes of law enforcement. In some circumstances, disclosures for the purposes of legal proceedings, particularly when an officer is required to disclose information to a court, will fall within a 'performance of functions and duties' exception. However, where, as a matter of policy, disclosures for the purposes of legal proceedings are desirable, it may be necessary to include an exception or information-handling provision to this effect in a specific secrecy provision.

With consent

10.90 A number of exceptions permit the disclosure of information with the consent of the person or entity to whom the information relates. Exceptions for the disclosure of information with consent generally appear in specific secrecy offences that concern the disclosure of personal, commercial or confidential information.[83] However, other secrecy laws that cover information of this kind, such as those regulating officers of the ATO, do not permit the disclosure of information with consent.[84]

---

81 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).

82 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).

83 See, eg, *Gene Technology Act 2000* (Cth) s 187(1)(f); *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(4)(b); *Australian Federal Police Act 1979* (Cth) s 60A(2C); *Reserve Bank Act 1959* (Cth) s 79A(3); *National Health Act 1953* (Cth) s 135A(8).

84 *Income Tax Assessment Act 1936* (Cth) s 16.

Submissions and consultations

10.91 In the *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions*, the Treasury noted that permitting the disclosure of information by the ATO with a taxpayer's consent would be in line with other secrecy laws.[85] In its submission to this Inquiry, the ATO observed that there would be 'administrative benefits if a taxpayer could consent to his or her information being released to a third party'.[86]

10.92 The Treasury submitted, 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.[87] 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 draft 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.[88]

ALRC's views

10.93 In Chapter 8, the ALRC expresses the view that the unauthorised disclosure of personal or commercial information does not, without more, warrant criminal sanctions under specific secrecy offences. Therefore, in the ALRC's view, specific secrecy offences would not generally require an exception allowing the disclosure of personal or commercial information with consent. In the absence of a specific secrecy offence, exceptions in the *Privacy Act 1988* (Cth) would allow an Australian Government agency to disclose personal information with the person's consent.[89]

10.94 However, as discussed in Chapter 8, specific secrecy offences that cover personal or commercial information may be warranted where regulatory agencies—such as taxation or social security agencies, and corporate regulators—receive large amounts of personal and commercial information. Here, the unauthorised disclosure of this information may not only harm a person's private interests, but may also cause harm to the public interest in the relationship of trust between the government and individuals which is integral to an effective regulatory system or the provision of government services.

---

85 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 27.

86 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

87 The Treasury, *Submission SR 22,* 19 February 2009.

88 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.15].

89 *Privacy Act 1988* (Cth) s 14, IPP 11.

10.95 In this context, it may be that the disclosure of personal or commercial information with the consent of the person or entity to whom the information relates would not cause the kind of harm to the public interest that these offences seek to prevent. The trust placed by an individual in the government—that it will not misuse personal or commercial information provided to it—is not breached where the person consents to the disclosure of their information.

10.96 The ALRC notes, however, that an exception for disclosures with consent was not included in the Tax Laws Exposure Draft Bill due to concerns about the validity of consent and to ensure 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'.[90]

10.97 In the ALRC's view, the appropriateness and form of exceptions to allow the disclosure of personal or commercial information with consent will depend on the context in which the specific secrecy offence operates. As such, the ALRC does not make any recommendations with respect to this exception.

To avert a serious threat to a person's life, health or safety

10.98 As noted in Chapter 3, some secrecy provisions contain exceptions permitting the disclosure of information in order to avert threats to a person's life, health or safety.[91] For example, s 19H of the *National Measurement Act 1960* (Cth) provides that a person commits an offence if he or she copies, makes a record of, uses or discloses protected information. However, the section also provides that this offence will not apply where:

> the person believes, on reasonable grounds, that the copying, recording, use or disclosure of the protected information is necessary for the purpose of preserving the safety of another person or other persons.[92]

10.99 A number of other exceptions that permit the disclosure of information to prevent a threat to a person's life, health or safety require the disclosure to be made or authorised by a senior officer.[93] For example, the *Child Support (Assessment) Act 1989* (Cth) provides that the secrecy offence:

---

90 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.16].

91 See, eg, *Child Support (Assessment) Act 1989* (Cth) s 150(3)(e); *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34(1A); *Customs Administration Act 1985* (Cth) s 16(3F).

92 *National Measurement Act 1960* (Cth) s 19H(3). Similar exceptions are included in, for example: *Australian Citizenship Act 2007* (Cth) s 43(1B); *Surveillance Devices Act 2004* (Cth) s 45(4); *Migration Act 1958* (Cth) s 366E(1A).

93 See, eg, *Dental Benefits Act 2008* (Cth) s 34(4); *Aged Care Act 1997* (Cth) s 86-3; *Child Support (Registration and Collection) Act 1988* (Cth) s 16(3); *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34(1A).

> does not prevent the Registrar or a person authorised by the Registrar from communicating any protected information: ...
>
> (e) to any person, if the information concerns a credible threat to the life, health or welfare of a person and either of the following applies:
>
> (i) the Registrar, or the person authorised by the Registrar, believes on reasonable grounds that the communication is necessary to prevent or lessen the threat;
>
> (ii) there is reason to suspect that the threat may afford evidence that an offence may be, or has been, committed against a person and the information is communicated for the purpose of preventing, investigating or prosecuting such an offence.[94]

10.100 In addition, the *Criminal Code* includes a defence of 'sudden or extraordinary 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.[95]

Submissions and consultations

10.101 Chapter 7 discusses a number of submissions that supported the inclusion of an exception for disclosures to prevent serious and imminent threats to life or health in the general secrecy offence.[96]

10.102 In addition, the CDSMAC expressed concerns about the limited operation of exceptions for disclosures necessary to prevent serious and imminent threats to life, health or safety in relation to child protection. In particular, the CDSMAC noted that exceptions, and the defence of 'sudden or extraordinary emergency' in the *Criminal Code,*[97] require a sense of immediacy and urgency—a high threshold to meet. In the context of child protection, the CDSMAC noted that:

> the threshold for release of information on public interest grounds adopted by Centrelink—whether the release of information is necessary to prevent or lessen a threat to health, safety or welfare of a person—has supported the release of information to Child Protection Agencies in the majority of cases, with only a small proportion of requests resulting in non-disclosure. Unlike some of the other legislative exceptions, and guidelines developed, this test does not require the threat to be either serious or imminent, but rather focuses on the necessity of the information to be released to reduce or lessen a relevant threat. The inclusion of 'welfare' as a ground for exception is particularly relevant to child protection issues.[98]

---

94 *Child Support (Assessment) Act 1989* (Cth) s 150(3).
95 *Criminal Code* (Cth) s 10.3. This defence is discussed in detail in Ch 7.
96 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009.
97 *Criminal Code* (Cth) s 10.3.
98 Community and Disability Services Ministers' Advisory Council, *Submission SR 80,* 28 August 2009.

10.103 DoHA submitted that the provision in the *Health Insurance Act,* which allows for the disclosure of information where there is a threat to the life or health of a person, was an important exception which should be retained.[99]

ALRC's views

10.104 In Chapter 7, the ALRC does not recommend that the general secrecy offence should include an exception to permit the disclosure of information to prevent or lessen a threat to a person's life, health or safety, on the basis that existing exceptions, such as disclosures with the authority of an agency head or minister, or the *Criminal Code* defence of sudden or extraordinary emergency, may be available. However, the ALRC considers that an exception of this kind may have a place in some specific secrecy offences where the *Criminal Code* defence would not be sufficient. For example, the *Criminal Code* defence may not encompass disclosures to prevent a threat to the 'welfare' of a person.

10.105 In Chapter 8, the ALRC recommends that specific secrecy offences should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest, except in certain limited circumstances.[100] An exception that permits the disclosure of information to avert a threat to a person's life, health or safety would require the person making the disclosure to balance this benefit against the likelihood and seriousness of the harm to the public interest identified in the offence.

10.106 In some cases, existing exceptions of this kind only permit a senior officer in an agency to disclose the information. In the ALRC's view, this is particularly appropriate where the decision to make a disclosure would require the balancing of important public interests.

10.107 Like many authorised disclosure provisions, the desirability and operation of exceptions to permit the disclosure of information in order to avert threats to a person's life, health or safety depend on the context in which they operate. As noted by the CDSMAC, there may be circumstances in which it is appropriate for exceptions of this kind to cover a person's welfare, as well as life, health or safety. For these reasons, the ALRC does not make any recommendations regarding the formulation or content of this exception.

Codification of authorised disclosures

10.108 As noted above, some secrecy offences include both general exceptions, such as disclosures in the performance of duties, and more prescriptive exceptions that

99 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.
100 Recommendation 8–2.

permit the disclosure of certain information for specified purposes or to specified persons or entities.

10.109 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.[101] In addition, the Secretary may disclose protected information in at least 12 separately defined circumstances,[102] 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'.[103]

10.110 In DP 74, the ALRC reached the preliminary view that expressing such provisions as exceptions to a secrecy offence is not always a necessary or desirable approach.[104] The ALRC considered that secrecy provisions might be simplified by relying on more generic exceptions, such as disclosure in the performance of a function or duty under an Act, or as required or authorised by law.[105] The ALRC proposed that specific secrecy offences that include extensive codification of permissible disclosures should be reviewed to establish whether these exceptions are necessary in view of the desirability of simplifying secrecy offences.[106]

Submissions and consultations

10.111 Civil liberties groups supported the general idea of simplifying disclosure provisions.[107] For example, Liberty Victoria submitted that this 'would seem to be best practice, and would enable Commonwealth officers to better understand when a disclosure is appropriate and acceptable'.[108]

10.112 However, a number of agencies submitted that detailed exceptions to specific secrecy offences were the most effective way to protect and share information in particular circumstances. For example, the Australian Prudential Regulation Authority noted that the exceptions in the *Australian Prudential Regulation Authority Act 1998* (Cth):

---

101 *Aged Care Act 1997* (Cth) s 86-2.

102 Ibid s 86-3.

103 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.

104 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), [11.35].

105 Ibid, [11.35].

106 Ibid, Proposal 11–2.

107 Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

108 Liberty Victoria, *Submission SR 50,* 5 August 2009.

> all fulfil distinct and important functions and should be retained. Any consideration of these specific exceptions would require careful consideration in order to avoid complicating established practice with regard to the handling of protected information.[109]

10.113 AUSTRAC submitted that detailed codification of permitted disclosures in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) was necessary with respect to AUSTRAC information:

> many of the provisions relate to those persons who expressly have access to AUSTRAC information (particularly under the AML/CTF Act as designated agencies). Twenty-four designated agencies or categories of designated agency, in addition to the Australian Taxation Office, are currently listed in the Act, each of which requires detail in regard to the relevant officer of the designated agency to which AUSTRAC information may be disclosed ... This is to provide certainty that sensitive information is disclosed at the appropriate level ...
>
> AUSTRAC considers that the simplification of such exceptions may create uncertainty as a broad application would not provide the required detail to ensure that sensitive information is disclosed in a manner that protects that information.[110]

10.114 Similarly, the ATO preferred an approach where secrecy provisions set out a general prohibition on the disclosure of taxpayer information, and then set out a range of exceptions to that prohibition:

> [T]he ATO considers that the specific exceptions to the tax law secrecy provisions, such as those permitting disclosures to other government agencies for particular purposes should be retained. While the performance of duties exception provides flexibility in the administration of the tax laws, the specific exceptions provide clarity and certainty for officers and taxpayers. The ATO believes that the current combination of the specific exceptions and the general performance of duties exception to the general prohibition on the disclosure of taxpayer information is the most appropriate approach with regard to taxation information.[111]

10.115 Some stakeholders referred to the decision of the High Court in *Johns v Australian Securities Commission* (*Johns*)[112] as a reason why secrecy offences need to be associated with comprehensive statutory exceptions.[113] In *Johns*, the High Court held 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

---

109 Australian Prudential Regulation Authority, *Submission SR 52,* 6 August 2009.
110 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.
111 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
112 *Johns v Australian Securities Commission* (1993) 178 CLR 408.
113 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009; The Treasury, *Submission SR 22,* 19 February 2009.

power is subject to a statutory duty of confidentiality, which means that the information may not be used or disclosed except as authorised by the statute.[114]

10.116 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 in s 155AAA of the *Trade Practices Act 1974* (Cth).[115]

10.117 The Treasury considered that provisions that permit sensitive information to be shared should be closely considered by the Parliament on a case-by-case basis:

> While general disclosure provisions (such as those permitting disclosures in the course of an officer's duties) are necessary and appropriate, Treasury considers that where (for instance) there is a need for other Government departments to access taxpayer information, this is best addressed on a case by case basis and in legislation. This procedure enables a careful analysis of the public interest in the disclosure and ensures that any move to permit disclosures is subject to the rigors of Parliamentary oversight.[116]

10.118 Finally, the AGD submitted 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'.[117] 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'.[118] Other agencies highlighted similar advantages to framing secrecy provisions in this way.[119]

ALRC's views

10.119 The ALRC considers that, in some circumstances, specific secrecy offences should codify authorised disclosures. This may be appropriate, for example, where the sensitive nature of the information requires that it be shared only within a tightly defined group of entities and for particular purposes—for example, as is the case with the statutory regime for sharing AUSTRAC information.

---

114 *Johns v Australian Securities Commission* (1993) 178 CLR 408, 424.

115 *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.

116 The Treasury, *Submission SR 60,* 10 August 2009.

117 Attorney-General's Department, *Submission SR 36,* 6 March 2009. The AGD also expressed reservations about the potential inflexibility of this approach.

118 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.

119 See, eg, 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.

10.120 In other situations, codification may supplement a 'performance of duties as an officer' exception. As discussed above, exceptions that permit the disclosure of information in the performance of an officer's duties are limited by the legislation governing the officer, and so may not permit the disclosure of information for purposes outside of those duties. Where this is the case, it may be necessary for specific secrecy offences, or authorised disclosure provisions, to codify other circumstances in which information may be shared.

10.121 Once again, because the formulation of such exceptions depends on the context of the secrecy offence, the ALRC does not make a recommendation in this area.

Form of authorised disclosure provisions

10.122 As noted at the beginning of this chapter, authorised disclosure provisions may be framed as exceptions or defences to secrecy offences, or as information-handling provisions that are not attached to a secrecy offence. Earlier in this chapter the ALRC recommends that, when reviewing specific secrecy offences for repeal, consideration should be given to whether any exceptions or authorised disclosure provisions should be retained in order to provide a legislative basis for information-sharing arrangements and to give content to the exceptions in the recommended general secrecy offence.

10.123 In Chapter 7, the ALRC sets out the differences between an exception and a defence. In summary, an 'exception' limits the scope of conduct prohibited by a secrecy offence, while a 'defence' may excuse conduct that is prohibited by a secrecy offence. In some circumstances, the distinction between an exception and a defence will be of limited significance, because the *Criminal Code* 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 burden.[120] The *Criminal Code* requires that, except in particular circumstances, or where an offence expressly provides otherwise, a burden of proof imposed on a defendant is an evidential burden only,[121] which means that the defendant must provide evidence to suggest a reasonable possibility that the defence is made out.[122] Once the defendant has met the evidential burden the prosecution must refute the defence and prove all elements of the offence beyond reasonable doubt.[123]

---

120 *Criminal Code* (Cth) s 13.3(3). Legislative 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).

121 *Criminal Code* (Cth) s 13.4.

122 Ibid s 13.3.

123 Ibid s 13 .1.

10.124 Some offences expressly impose a legal burden of proof on the defendant,[124] which requires the defendant to establish the defence on the balance of probabilities. The prosecution must then disprove the defence beyond reasonable doubt.[125]

10.125 The *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (*Guide to Framing Commonwealth Offences*) issued by the AGD provides that:

> a matter should only be included in a defence, thereby placing the onus on the defendant 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.[126]

10.126 As noted above, specific secrecy offences generally contain exceptions rather than defences. In DP 74, the ALRC proposed that 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,* and consideration should be given to recasting the provision as an exception, rather than as a defence.[127]

Submissions and consultations

10.127 While only a few stakeholders commented on this issue, those that did so supported the ALRC's proposal.[128] Indigenous Business Australia (IBA) noted that the secrecy offence in the *Aboriginal and Torres Strait Islander Act 2005* (Cth) (ATSI Act) includes a defence, and submitted that:

> The ATSI Act places the onus on individual officers and staff of IBA to establish a defence to any prosecution for the disclosure of information relating to home or business loans. This is unreasonable and contributes to organisational and staff aversion in relation to information handling.[129]

10.128 In response to IP 34, the Law Council of Australia noted that there are procedural disadvantages in criminal prosecutions for a defendant who claims a defence rather than being able to rely on an exception.[130]

---

124 Ibid s 13.4. See, eg, *Crimes Act 1914* (Cth) s 79(5) and (6) for examples of secrecy offences in which the defendant bears a legal burden of proof.

125 *Criminal Code* (Cth) s 13.5.

126 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 28–29.

127 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 11–1.

128 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

129 Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

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

ALRC's views

10.129 In practice, while exceptions are commonly included in Commonwealth secrecy laws, only a few secrecy offences expressly provide defences. Rather than attempting to protect legitimate disclosures through a 'defence' that arises after a person has been found to satisfy all the elements of the offence, the ALRC's preference is for specific secrecy offences to be framed in such a way that they do not encompass legitimate disclosures in the first place. In the ALRC's view, the inclusion of a requirement that the disclosure cause, or is likely or intended to cause, harm to an essential public interest is one way in which specific secrecy offences will be limited to legitimate conduct.

10.130 However, the ALRC recognises that, in some circumstances, criminal law policy will require a matter to be framed as an exception or a defence, for example where it would be significantly more difficult for the prosecution to disprove an element of the offence than it would for the defendant to establish it. Exceptions and defences to specific secrecy offences should be framed consistently with the policies in the *Guide to Framing Commonwealth Offences.*

Recommendation 10–4 Exceptions and defences in specific secrecy offences should be framed consistently with the principles set out in the *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*.

Public interest disclosure

10.131 As discussed in Chapter 2, the Terms of Reference to this Inquiry require the ALRC to consider the way in which secrecy laws interact with other laws and practices, including those relating to public interest disclosures, or 'whistleblowing'.[131]

10.132 There is currently limited protection at the Commonwealth level for people who make public interest disclosures. Section 16 of the *Public Service Act* provides very limited protections for an Australian Public Service (APS) employee who has reported breaches of the APS Code of Conduct to specified bodies. As noted in Chapter 2, this provision does not provide immunity from criminal liability under secrecy laws.

10.133 Some Commonwealth legislation contains 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

131 The Terms of Reference are set out at the beginning of this Report.

framework in the Act) regarding the assault of a person in residential care.[132] The *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) provides 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'.[133]

10.134 As discussed in more detail in Chapter 2, the House of Representatives Standing Committee on Legal and Constitutional Affairs (the Standing Committee) has recommended that the Australian Government introduce legislation—the Public Interest Disclosure Bill—to provide 'whistleblower' protections in the Australian Government public sector.[134]

10.135 In summary, the Standing Committee recommended that a broad range of Australian Government officials[135] be able to make public interest disclosures about 'serious matters'[136] 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 protection, including immunity from: criminal liability (including under secrecy offences); civil liability; and administrative sanctions.[137]

10.136 In addition, the Standing Committee recommended that protection extend to a person who makes a disclosure to external third parties, for example, 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.[138]

ALRC's views

10.137 The ALRC considers that it is important that public interest disclosure legislation cover the same people subject to secrecy offences. If not, there is a risk that a whistleblower would still be subject to prosecution for contravention of a secrecy offence.

10.138 In Chapter 7, the ALRC recommends that, in order to provide effective protection for whistleblowers, public interest disclosure legislation should cover the same categories of people subject to the general secrecy offence and the subsequent

---

132 *Aged Care Act 1997* (Cth) s 96-8.
133 *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) pt 10-5.
134 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.
135 Ibid, Rec 3.
136 Ibid, Rec 7.
137 Ibid, Rec 14.
138 Ibid, Rec 21.

disclosure offence for the unauthorised disclosure of information received from a Commonwealth officer on terms requiring it to be held in confidence.[139]

10.139 Specific secrecy offences, however, apply to a broad range of people, including Commonwealth officers, individuals providing services for or on behalf of the Commonwealth or engaged in federally funded or regulated areas of the private sector, and state, territory or local government employees. A significant number of specific secrecy offences apply to 'any person'.[140]

10.140 While the proposed public interest disclosure legislation will cover a broad range of Australian government officials, the Standing Committee did not recommend that the legislation cover 'any person'. It may be possible to provide protection for some individuals by way of a deeming provision. The Standing Committee 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 disclosure.[141]

10.141 In the ALRC's view, one consideration in making a decision whether to deem a person to be a 'public official' for the purposes of public interest disclosure legislation should be whether the person is subject to a secrecy offence. Alternatively, in some areas of government activity or regulation, it may be appropriate to establish public interest disclosure regimes targeted to the requirements of people working within that sector.

Recommendation 10–5 In developing public interest disclosure legislation the Australian Government should ensure that, where possible, the legislation protects individuals subject to specific secrecy offences.

Override provisions

10.142 Some Commonwealth legislation includes provisions that purport to override the secrecy provisions in other legislation. For example, the *Ombudsman Act 1976* (Cth) confers power on the Ombudsman to obtain information relevant to an investigation.[142] The Act provides that:

---

139 Recommendation 7–3.

140 The range of parties regulated by specific secrecy offences is discussed in Ch 9.

141 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.

142 *Ombudsman Act 1976* (Cth) s 9.

> Notwithstanding the provisions of any enactment, a person is not excused from furnishing any information, producing a document or other record or answering a question when required to do so under this Act on the ground that the furnishing of the information, the production of the document or record or the answer to the question would contravene the provisions of any other enactment (whether enacted before or after the commencement of the *Prime Minister and Cabinet Legislation Amendment Act 1991*).[143]

10.143 Section 30 of the *Auditor-General Act 1997* (Cth), while differently worded, is intended to have a similar effect. It provides that the operation of the Auditor-General's information-gathering powers 'is not limited by any other law (whether made before or after the commencement of this Act), except to the extent that the other law expressly excludes the operation of' those sections of the Act relating to the Auditor-General's information-gathering powers.[144]

10.144 In Chapter 16, the ALRC recommends that the FOI Act should be amended to expressly override secrecy obligations in other legislation.[145]

10.145 A general principle of statutory interpretation is that a later statute will, by implication, repeal an earlier, inconsistent statute. Override provisions of this kind represent an attempt to limit the ability of later legislation to impliedly repeal an earlier Act. However, courts generally do not interpret the override provisions in this way, on the basis that an earlier Act should not bind a parliament's ability to pass later inconsistent legislation.[146] Therefore, a secrecy provision enacted after the enactment of a statute with an override provision, such as the *Ombudsman Act*, arguably will still apply despite the override provision in the earlier Act.

10.146 It is, however, generally acknowledged that some Commonwealth legislation will override secrecy provisions in other legislation. For example, the Explanatory Material accompanying the Tax Laws Exposure Draft Bill states that there are a 'number of non-taxation Acts which effectively override the secrecy and disclosure provisions contained in the [taxation secrecy] framework'.[147] The Explanatory Material lists provisions of this kind—including provisions in the *Ombudsman Act, Auditor-General Act,* and *Inspector-General of Taxation Act 2003* (Cth)—and notes that most of these provisions have the effect that, if a taxation officer is compelled to provide

---

143 Ibid s 9(4).

144 Other provisions which may override secrecy provisions include: *Water Act 2007* (Cth) s 239; *Anti-Terrorism Act (No 2) 2005* (Cth) sch 6; *Inspector-General of Taxation Act 2003* (Cth) s 15; *Privacy Act 1988* (Cth) s 44. The interaction between secrecy provisions and the *Freedom of Information Act 1982* (Cth) and parliamentary privilege are discussed in Ch 16.

145 Recommendation 16–4.

146 D Pearce and R Geddes, *Statutory Interpretation in Australia* (5th ed, 2001), [7.14] citing *South-Eastern Drainage Board (SA) v Savings Bank of South Australia* (1939) 62 CLR 603. See also *Kartinyeri v Commonwealth* (1998) 195 CLR 337, [13]–[14], [48].

147 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [1.27].

taxpayer information, they cannot be prosecuted for any offence contained within the tax secrecy framework.[148]

10.147 In addition, a generally phrased 'performance of duties' exception in a specific secrecy offence will permit the disclosure of information to a body with information-gathering powers. As stated in the context of reg 35 of the now repealed *Public Service Regulations 1935* (Cth):

> If an officer is required, by a body having legal authority to obtain information compulsorily, to give information or disclose the contents of documents which he has in his official capacity, it is in the course of his official duty to obey the requirement.[149]

Submissions and consultations

10.148 In a submission to this Inquiry, the IBA and the Commonwealth Ombudsman raised concerns that secrecy provisions prevented the provision of information to integrity and oversight agencies, such as the Ombudsman and the Auditor-General.

10.149 IBA noted that transparency and accountability were important to maintain stakeholders' confidence in government. In this context, the IBA was concerned that:

> Section 191 of the ATSI Act currently severely restricts the capacity of IBA to provide information, including to its portfolio Minister, agencies with responsibility for over-sighting Commonwealth administrative practices, such as the Ombudsman and Privacy Commissioner, Commonwealth agencies working in joint initiatives with IBA (such as FaHCSIA). IBA considers that the provisions are unduly restrictive and do not represent an appropriate balance between the need to protect confidential information and competing public interests.[150]

10.150 The Commonwealth Ombudsman described a situation in which secrecy provisions prevented an agency providing information to it for the purposes of an investigation:

> As part of our investigation, we sought information from the agency that was the subject of the complaint ...
>
> The agency refused to provide us with the information sought on the basis that it had obtained legal advice to the effect that the secrecy provisions of its enabling legislation overrode the *Ombudsman Act*. The legal advice included consideration of statutory interpretation principles as to whether a later Act repeals earlier inconsistent

---

148 Ibid.

149 *Mobil Oil Australia Pty Ltd v Commissioner of Taxation* (1963) 113 CLR 475, 505. Regulation 35 provided that 'except in the course of official duty, no information concerning public business or any matter of which an officer has knowledge officially shall be given, directly or indirectly, nor shall the contents of official papers be disclosed, by an officer or employee without the express authority of the Secretary'.

150 Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

> Acts and a commentary about resulting uncertainty in scenarios where some provisions of the *Ombudsman Act* providing for access to information might override the secrecy provisions of the other legislation but other provisions might not.[151]

10.151 The Ombudsman concluded that:

> Operating in an environment of uncertainty as to whether the access provisions of the Ombudsman Act might or might not override specific secrecy provisions in other Acts, is not conducive to this office fulfilling its statutory role of promoting good and accountable public administration. For this reason we would prefer a solution that makes it abundantly clear that our powers of access take precedence, unless the other Act specifically says that it overrides the *Ombudsman Act*.[152]

ALRC's views

10.152 The policy behind the override provisions in the *Ombudsman Act* and similar legislation is to facilitate the provision of all relevant information to integrity and investigatory agencies for the purposes of investigations. Specific secrecy offences should not preclude the provision of information to the Ombudsman, except on the basis of a clear parliamentary intention. Similar arguments apply in relation to the provision of information to other integrity agencies, such as the Auditor-General.

10.153 While there are benefits to using override provisions to indicate an intention that the provision of information to certain bodies or for particular purposes is not precluded by specific secrecy offences, the legal interpretation of such provisions has limited the effectiveness of override provisions, and accordingly, more may be needed to achieve this outcome. In particular, specific secrecy provisions should include exceptions that are broad enough to encompass the provision of information to bodies with power to obtain that information. As noted above, a generally expressed exception that permits the disclosure of information in the course of an officer's functions and duties has been held to permit the disclosure of information in such circumstances.

10.154 The ALRC recommends that specific secrecy provisions should generally include an exception for disclosures in the course of an officer's functions or duties.[153] Where it is necessary for a performance of duties exception to be more narrowly confined—for example, to the performance of duties under particular legislation—consideration should be given to how an exception of this kind will interact with laws which confer a power on bodies such as integrity agencies to acquire information for the purposes of investigations. In Chapter 11, the ALRC recommends that the *Guide to Framing Commonwealth Offences* should include guidance on the drafting of secrecy offences.[154] This should include guidance on the interaction between secrecy provisions and override provisions in other legislation.

---

151 Commonwealth Ombudsman, *Submission SR 20,* 19 February 2009.
152 Ibid.
153 Recommendation 10–2.
154 Recommendation 11–2.

11. Specific Secrecy Offences: Review and Guidance

Contents

Introduction

11.1 The ALRC's recommendations in Chapters 8, 9 and 10, form a set of principles to guide the creation of new specific secrecy offences and the review of existing offences. This chapter considers ways in which these principles can be applied to the 358 specific secrecy offences that the ALRC has identified on the Commonwealth statute book and to the development of new secrecy offences in the future.

Reviewing specific secrecy offences

11.2 Concerns have been raised about the number and diversity of Commonwealth secrecy provisions and the lack of consistency in the drafting of offences and associated penalties.[1] The Terms of Reference for this Inquiry ask the ALRC to report on options for ensuring a consistent approach across the Australian Government to the protection of Commonwealth information.[2]

11.3 In this Report, the ALRC makes a number of recommendations for the reform of specific secrecy offences. In the ALRC's view, applying these recommendations to existing secrecy offences will involve consideration of three interrelated issues:

---

1 See, eg, Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [5.118]; 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.

2 The Terms of Reference are set out at the front of this Report.

- does the conduct covered by the specific secrecy offence warrant the imposition of criminal sanction;

- do the terms of the specific secrecy offence comply with the best practice principles set out in Chapters 8, 9 and 10; and

- could the secrecy obligations within an Act or an agency's portfolio legislation be consolidated in a clear and accessible way?

11.4 This section discusses each of these three questions in turn. In doing so, it provides examples of specific secrecy offences that could be considered for amendment or repeal. The ALRC does not suggest that the specific secrecy offences considered here are the only offences that require review—rather, the examples are intended to demonstrate possible outcomes of the application of the recommendations of this Report to existing specific secrecy offences.

Are criminal sanctions warranted?

11.5 A threshold question in reviewing specific secrecy offences is whether it is appropriate for a breach of the secrecy provision to attract criminal sanctions. In Chapter 4, the ALRC sets out a framework for the reform of secrecy provisions. The framework reserves criminal penalties for conduct of such seriousness that it is likely to cause harm to essential public interests.

11.6 As noted in Chapter 3, a large number of specific secrecy offences deal only with the disclosure of personal or commercial information. In Chapter 5, the ALRC expresses the view that the unauthorised disclosure of personal and commercial information does not, without more, warrant the imposition of criminal sanctions. Where personal or commercial information is disclosed in the private sector, the matter may give rise to contractual, common law or equitable remedies, not criminal prosecution. The ALRC considers that, where personal or commercial information is disclosed in the public sector, similar options for redress should generally be available, including lodging a complaint under the *Privacy Act 1988* (Cth), the imposition of administrative penalties such as those provided by the *Public Service Act 1999* (Cth), as well as contractual, common law and equitable remedies.

11.7 The limited exception to this principle, discussed in Chapter 8, is where regulatory agencies—such as taxation or social security agencies or oversight bodies such as corporate regulators—need to strictly control sensitive personal and commercial information provided to them by the public. In these cases, the harm caused by the unauthorised disclosure of such information is to the public interest in maintaining the relationship of trust between the government and individuals that is integral to an effective regulatory system or the provision of government services.

11.8 Several specific secrecy offences impose criminal sanctions on a Commonwealth officer for the unauthorised disclosure of personal or commercial information.

Example: Section 60(1) of the *Age Discrimination Act 2004* (Cth)

Section 60(1) of the *Age Discrimination Act* provides that:

> A person bound by this section because of office, employment or authorisation must not, either directly or indirectly:
>
> (a) make a record of, or divulge or communicate to any person, any information relating to the affairs of another person acquired by the first-mentioned person because of that person's office or employment under or for the purposes of this Act or because of that person being or having been so authorised; or
>
> (b) make use of any such information as is mentioned in paragraph (a); or
>
> (c) produce to any person a document relating to the affairs of another person given for the purposes of this Act.
>
> Penalty: Imprisonment for 2 years.

This provision does not expressly state the harm sought to be prevented by the criminal offence. However, it is likely that the policy reasons for the offence are: first, to protect personal privacy; and secondly, to reassure people making a complaint of discrimination that the information that they provide will be treated confidentially.

The imposition of criminal sanctions for disclosures of personal information, or information that may affect civil or administrative processes, such as the investigation and resolution of a complaint of unlawful discrimination, is, in the ALRC's view, unwarranted.[3]

Consideration should be given to repealing this offence provision, or perhaps recasting it as a provision the breach of which would attract administrative penalties.

3 This issue is discussed in detail in Ch 5.

11.9 The ALRC has identified a number of similar offences, which criminalise the unauthorised disclosure, by Commonwealth officers, of personal or commercial information outside the core regulatory and oversight contexts discussed in Chapter 8.[4]

Submissions and consultations

11.10 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC made a number of proposals in relation to a review of specific secrecy offences in accordance with the proposals set out in DP 74.[5]

11.11 In a submission to this Inquiry, Ron Fraser supported the ALRC's approach to identifying specific secrecy offences for amendment or repeal. He noted that:

> It is particularly important that individual secrecy provisions applying to information relating to the affairs of persons ... should be repealed, and not replaced by provisions that encompass personal privacy and business affairs information.[6]

11.12 While some government agencies expressed in-principle support for reviewing specific secrecy offences, many noted that any such review must take account of the particular policy contexts and purposes of each specific offence. For example, the Australian Bureau of Statistics (ABS) was

> not opposed to comprehensive testing of secrecy provisions to determine which ones can be repealed and replaced with a general secrecy offence, and which ones should be retained as specific secrecy provisions. The ABS would expect to contribute to the testing process regarding the secrecy provisions in the [*Census and Statistics Act 1905* (Cth)].[7]

11.13 Similarly, the Australian Crime Commission (ACC) submitted that:

> Review of this profusion of legislation against suitable benchmarks is no doubt warranted, but it should be noted that the varying circumstances in which, and

---

4 See, eg, *Wheat Export Marketing Act 2008* (Cth) s 74; *Wheat Export Marketing (Repeal and Consequential Amendments) Act 2008* (Cth) sch 3 item 6; *AusCheck Act 2007* (Cth) s 15; *Offshore Petroleum and Greenhouse Gas Storage Act 2006* (Cth) s 758; *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 191; *Medical Indemnity Act 2002* (Cth) s 77; *Comprehensive Nuclear Test Ban Treaty Act 1998* (Cth) s 74(2); *Chemical Weapons (Prohibition) Act 1994* (Cth) s 102(2); *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63(3B); *Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992* (Cth) s 25; *Development Allowance Authority Act 1992* (Cth) s 114; *Disability Discrimination Act 1992* (Cth) s 127; *Export Finance and Insurance Corporation Act 1991* (Cth) s 87(5); *Australian Postal Corporation Act 1989* (Cth) ss 90H, 90LB; *Privacy Act 1988* (Cth) s 96; *Australian Human Rights Commission Act 1986* (Cth) s 49; *Dairy Produce Act 1986* (Cth) sch 2 cl 43; *Australian Trade Commission Act 1985* (Cth) s 94; *Sex Discrimination Act 1984* (Cth) s 112; *Environment Protection (Alligator Rivers Region) Act 1978* (Cth) ss 31(2), (4); *Social Welfare Commission (Repeal) Act 1976* (Cth) s 8; *Racial Discrimination Act 1975* (Cth) s 27F(1); *Trade Practices Act 1974* (Cth) s 10.89; *National Measurement Act 1960* (Cth) s 19H; *Migration Act 1958* (Cth) ss 377, 439.

5 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 12–4.

6 R Fraser, *Submission SR 78,* 21 August 2009.

7 Australian Bureau of Statistics, *Submission SR 58,* 7 August 2009.

> purposes for which, information is acquired may dictate a variety of approaches and uniformity should not be imposed arbitrarily.[8]

11.14 Some government agencies submitted that they needed their own specific secrecy provision on the basis that their provisions differed in significant and necessary ways from the general secrecy offence. For example, the Australian Taxation Office (ATO) considered that:

> the general secrecy offence differs significantly from the existing tax secrecy provisions, such that the general offence would not of itself provide sufficient protection for taxpayer information. As a result, the ATO strongly supports the retention of the tax law secrecy provisions.[9]

11.15 Similarly, the Department of Health and Ageing (DoHA) considered that health information was a special category of information that warranted specific protection:

> Health information collected in the course of administering health programs may be extremely sensitive and may need to continue to be protected by a specific secrecy provision, regardless of a general secrecy offence. In addition, specific secrecy offence provisions may still be appropriate to regulate certain conduct which would otherwise fall outside of the scope of the general secrecy offence (eg soliciting).[10]

11.16 Finally, the Australian Transaction Reports and Analysis Centre (AUSTRAC) submitted that AUSTRAC information needs to be protected for reasons beyond the harm to public interests identified in the general secrecy offence, and that the current secrecy provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) should be retained.[11]

Applying best practice principles

11.17 In Chapter 8, the ALRC recommends that, to avoid unnecessary replication of the general secrecy offence, specific secrecy offences should differ in significant and justifiable ways from the recommended general secrecy offence.[12] There may be legitimate reasons why a specific secrecy offence is necessary in some circumstances, for example where:

- the unauthorised disclosure causes, or is likely or intended to cause, harm to an essential public interest not covered by the general secrecy offence;
- the offence regulates people other than Commonwealth officers as defined in the general secrecy offence;

---

8 Australian Crime Commission, *Submission SR 75,* 19 August 2009.
9 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
10 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.
11 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.
12 Recommendation 8–3.

- the offence covers conduct other than the disclosure of information—such as soliciting, obtaining or making a record of information; or

- the penalties differ significantly from those provided by the general secrecy offence.

11.18 The extent to which these differences may justify the creation or retention of specific secrecy offences depends on the policy context for each offence.

11.19 In this Report, the ALRC makes a number of recommendations to guide the framing of specific secrecy offences. In summary, these recommendations provide that specific secrecy offences:

- should include an express requirement that, for an offence to be committed, the unauthorised disclosure caused, or was likely or intended to cause, harm to an identified essential public interest, except in certain limited circumstances (Recommendation 8–2);

- that apply to individuals other than Commonwealth officers, should clearly identify the parties regulated by the offence (Recommendation 9–1);

- that apply to Commonwealth officers, should also apply to former Commonwealth officers (Recommendation 9–2);

- should not extend to conduct other than the disclosure of information—such as making a record of, receiving or possessing, information—unless such conduct would cause, or is likely or intended to cause, harm to an essential public interest (Recommendation 9–3);

- should generally require intention as the fault element for the physical element consisting of conduct (Recommendation 9–4);

- with an express harm requirement, should generally require that a person knew, intended that, or was reckless as to whether, the conduct would cause harm to an essential public interest (Recommendation 9–5);

- without an express harm requirement, should require that a person knew, or was reckless as to whether, the protected information fell within a particular category, and should not provide that strict liability applies to that circumstance (Recommendation 9–6);

- should provide maximum penalties that reflect the seriousness of the potential harm caused by the unauthorised conduct, and the fault elements that attach to the elements of the offence (Recommendation 9–8);

- that impose secrecy obligations on officers, should generally include an exception for disclosures in the course of an officer's functions or duties (Recommendation 10–2); and

- should not apply to the disclosure of information that is lawfully in the public domain (Recommendation 10–3).

11.20 Where an existing specific secrecy offence is warranted, it should be reviewed for compliance with these best practice principles.

Submissions and consultations

11.21 As noted above, in DP 74 the ALRC proposed that the Australian Government review specific secrecy offences in accordance with its proposals.[13]

11.22 A number of stakeholders supported a review of secrecy provisions against best practice principles,[14] to remove duplication and reduce the number of secrecy provisions.[15] However, the Department of Human Services (DHS) submitted that a whole of government review of secrecy provisions would take considerable time, and noted that:

> The Human Services Portfolio will continue to work with other Commonwealth Departments, with State and Territory governments and with the Office of the Privacy Commissioner to look for ways to remove secrecy and related privacy impediments to improved service delivery while maintaining appropriate levels of protection for personal and business and professional information.[16]

11.23 Some agencies noted that reviews of secrecy provisions in particular portfolios were imminent or currently underway. For example, the Treasury and the ATO referred to a review of taxation secrecy laws, discussed further below.[17] The Department of Defence also noted that it was undertaking a review of offence provisions in pt VII of the *Defence Act 1903* (Cth), including specific secrecy offences:

---

13 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 12–4.

14 R Fraser, *Submission SR 78,* 21 August 2009; Australian Privacy Foundation, *Submission SR 71,* 16 August 2009; Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

15 Australia's Right to Know, *Submission SR 72,* 17 August 2009; Community and Public Sector Union, *Submission SR 57,* 7 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

16 Department of Human Services, *Submission SR 83,* 8 September 2009.

17 The Treasury, *Submission SR 60,* 10 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009. See Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth); The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006).

> The review will aim to modernise the offence provisions, bring them into line with current Commonwealth criminal law policy and address overlap with other Commonwealth criminal offences.[18]

11.24 Two stakeholders considered that it would be appropriate for the ALRC to recommend a timeframe for agencies to review specific secrecy offences. For example, Ron Fraser stated that it would be appropriate to include

> a requirement that all individual secrecy provisions should be so reviewed within, say, three years of government acceptance of its report on secrecy. It might also be advisable to makes some suggestions as to an appropriate lead agency or agencies for such an exercise, perhaps the Information Commissioner if established, subject to specific funding for the project. Otherwise, there seems a danger that the whole exercise could drift on for many years.[19]

11.25 Similarly, the Australian Privacy Foundation commented that:

> We support the Commission's proposals for systematic review of all existing specific secrecy provisions to justify why they are necessary over and above the proposed new general provision ... However we would be very concerned if there were no timescales attached—leaving timing to agencies would invite lengthy delays.[20]

11.26 Some stakeholders suggested that there was a risk in repealing specific secrecy laws. For example, the Australian Privacy Foundation noted that:

> One possible downside of repealing secrecy provisions in individual laws and relying on a single provision in the Criminal Code is that the secrecy 'mandate' is less visible/transparent to anyone reading a particular law. But on balance it should be possible to compensate for this with education, confidentiality agreements, contractual provisions etc. We submit that the Commission should recommend vigorous promotion of generic secrecy obligations to Commonwealth public servants by all relevant means.[21]

Consolidation of specific secrecy offences

11.27 The potential to consolidate specific secrecy offences may also be considered by agencies when reviewing specific secrecy offences.

11.28 In some instances, consolidation of secrecy offences within a statute may be desirable in order to promote consistency and accessibility of law. However, the Australian Government Attorney-General's Department (AGD) *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (*Guide to Framing Commonwealth Offences*) sets out the principle that offences should generally be located with other provisions with the same substantive subject matter, rather than being grouped together in an 'Offences' part:

---

18 Department of Defence, *Submission SR 69,* 14 August 2009.
19 R Fraser, *Submission SR 78,* 21 August 2009.
20 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.
21 Ibid. See also Community and Public Sector Union, *Submission SR 57,* 7 August 2009.

> 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.[22]

11.29 Secrecy provisions in related pieces of legislation administered by the same agency may also be consolidated into a single Act. For example, in 2006, the Treasury undertook to review secrecy and disclosure provisions across all taxation legislation (the Taxation Secrecy Review). In its *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions*, the Treasury noted that taxation secrecy provisions are located in numerous different Acts, differ in their language and scope, and have inconsistent penalties.[23] Further, it noted that some provisions merely duplicated provisions located in other Acts.[24]

11.30 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 Number disclosures—be standardised and consolidated into a single piece of legislation.[25]

11.31 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 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.[26]

11.32 In DP 74, the ALRC proposed that the Australian Government review secrecy offences with a view to consolidation, where possible, into a single provision or part in an Act or regulation, or one Act where multiple secrecy provisions exist across several acts for which the same agencies are responsible.[27]

---

22 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007), 13.

23 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), [2.1].

24 Ibid.

25 Ibid, [2.3].

26 Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [1.04]–[1.18].

27 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 12–3.

Submissions and consultations

11.33 A number of stakeholders indicated support for the consolidation of secrecy provisions.[28] For example, Liberty Victoria commented that it:

> supports consolidating retained secrecy provisions as it would not only be best practice, but would make their application by Commonwealth officers more practicable and therefore increase compliance.[29]

11.34 While most stakeholders agreed that the consolidation of secrecy provisions, where possible, is a desirable outcome, some stakeholders emphasised that consolidation is not always appropriate.[30] The AGD observed that, while consolidation of secrecy laws may help to reduce complexity in some cases, its effectiveness would depend upon the objectives and overall drafting of each Act.[31]

11.35 The ACC also noted the importance of the legislative context:

> integration or co-location of offences of a similar character may be desirable from the viewpoint of understanding the secrecy aspects of the legislation as a whole but removing them from their legislative context may make it harder for the reader to understand how the legislation works in relation to a particular procedure or subject matter.[32]

11.36 The Department of Education, Employment and Workplace Relations noted both the benefits and limitations of consolidating secrecy provisions:

> 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.[33]

11.37 DoHA did not consider that it would be appropriate to consolidate secrecy provisions where the secrecy provisions apply to different persons, protect different

---

28 Australia's Right to Know, *Submission SR 72,* 17 August 2009; Community and Public Sector Union, *Submission SR 57,* 7 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

29 Liberty Victoria, *Submission SR 50,* 5 August 2009.

30 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.

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

32 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

33 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.

kinds of information and attract different penalties. It noted that this was 'more likely to create confusion than increase clarity'.[34]

11.38 The Australian Intelligence Community (AIC) acknowledged that 'consolidation of existing secrecy provisions could simplify arrangements', but 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. … these provisions are set out clearly and logically, in the context of those Acts.[35]

11.39 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'.[36] 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.[37]

11.40 In response to the Issues Paper, *Review of Secrecy Laws*,[38] 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.
- 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.[39]

11.41 In response to DP 74, the Treasury noted that:

> The Tax Secrecy Bill, in bringing together exceptions to non-disclosure found across the taxation law provides an extensive list of the circumstances in which taxpayer information can be lawfully disclosed. As part of the process of bringing these exceptions together, Treasury has been conscious of the need to both simplify them where possible but also to ensure that the consolidation/simplification process does

---

34 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.
35 Australian Intelligence Community, *Submission SR 37,* 6 March 2009.
36 Australian Commission for Law Enforcement Integrity, *Submission SR 18,* 18 February 2009.
37 Department of Human Services, *Submission SR 26,* 20 February 2009.
38 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008).
39 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

> not come at the expense of a significant expansion of the circumstances in which information can be disclosed.[40]

11.42 The ATO also referred to the consolidation of tax secrecy provisions and submitted that 'where similar rationale exists in other legislative schemes, the ATO is supportive of retaining separate secrecy provisions to protect distinct types of information or access to information where this should be regulated'.[41]

ALRC's views

11.43 The ALRC considers that reviewing specific secrecy offences to determine, first, whether any should be repealed on the basis that criminal sanctions are not warranted, and secondly, against the principles recommended in Chapters 8, 9 and 10, would ensure that specific secrecy offences only target the disclosure of Commonwealth information where it harms essential public interests. It would also increase the consistency between secrecy offences, reduce complexity and make the law more accessible.

11.44 While the practicalities of consolidating secrecy provisions would depend on the objectives and drafting of specific legislation, the ALRC considers that the consolidation of secrecy provisions into a single provision or part in an Act or regulation assists people subject to secrecy provisions to identify and understand their obligations to protect certain information. Where secrecy offences exist across a number of statutes administered by the same agency, the Review of Taxation Secrecy Laws provides a good model for reviewing specific secrecy offences with an eye to consolidation. The ALRC considers that this kind of exercise might usefully be repeated where secrecy provisions across related legislation seek to protect similar kinds of information.

11.45 The ALRC acknowledges that the implementation of the ALRC's recommendations for reform of specific secrecy offences will be a lengthy and complex process. Each of the three considerations outlined above will involve a detailed review of the policy, purpose and legal effect of each secrecy offence.

11.46 As noted above, several agencies are currently reviewing the secrecy offences in their portfolio legislation. The ALRC anticipates that there will be ongoing opportunities for other agencies to review secrecy offences. In some cases, an agency may undertake a review of secrecy offences across the statutes for which the agency has responsibility—as in the case of the recent review of taxation secrecy provisions undertaken by the Treasury.[42] In other cases, review might be more opportunistic—for

---

40 The Treasury, *Submission SR 60,* 10 August 2009.

41 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

42 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).

example when other amendments to legislation are being contemplated or when new legislation is being drafted.

11.47 Because of the complexity of the task, and because many reviews will extend across different government agencies, the ALRC is not recommending a timeframe for the review of specific secrecy offences.

Recommendation 11–1 Australian Government agencies should review specific secrecy offences to determine:

(a) whether a criminal offence is warranted;

(b) if so, whether the secrecy offence complies with the best practice principles set out in Recommendations 8–1 to 8–3, 9–1 to 9–9 and 10–1 to 10–4; and

(c) whether it would be appropriate to consolidate secrecy offences into:

  (i) a single provision or part where multiple secrecy provisions exist in the same Act; or

  (ii) one Act where secrecy offences exist in more than one Act for which the same Australian Government agency is responsible.

Policy guidance and drafting directions

11.48 The AGD has a central role in developing and implementing criminal law policy. 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. It scrutinises all offence, civil penalty and law enforcement provisions in proposed legislation and provides policy advice and assistance to agencies developing such provisions.[43] As part of this role, the AGD has produced the *Guide to Framing Commonwealth Offences*,[44] which consolidates the principles and precedents relevant to the framing of offences and enforcement provisions in Commonwealth laws.

43 Attorney-General's Department, *Organisational Structure: Criminal Law and Law Enforcement Branch* (2009) <www.ag.gov.au/www/agd/agd.nsf/Page/OrganisationalStructure_CriminalLawBranch> at 30 November 2009.

44 Australian Government Attorney-General's Department, *A Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* (2007).

11.49 Drafting directions are instructions issued by the head of the Office of the Parliamentary Counsel. The principal function of the Office of Parliamentary Counsel is to draft bills for introduction into Parliament and draft amendments to bills. All drafters are required to comply with drafting directions, to help ensure consistency.[45]

11.50 Drafting directions already cover some aspects of drafting secrecy provisions. *Drafting Direction No. 3.5* 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.[46]

11.51 *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.[47]

11.52 In DP 74, the ALRC proposed that the AGD should incorporate guidance in the *Guide to Framing Commonwealth Offences* on: the circumstances in which the enactment of a specific secrecy offence may be justified; the drafting of secrecy offences; and benchmark penalties.[48] While only a few stakeholders commented on these proposals, those that did so, supported them.[49]

ALRC's views

11.53 The recommendations made by the ALRC in this Report are intended to establish a principled basis for the drafting of secrecy provisions, based on an understanding of the appropriate relationship between the public interests protected by secrecy and the public interests in open and accountable government and freedom of expression.

11.54 There is a need, in this regard, for both general policy guidance, including in relation to when the enactment of a specific secrecy offence may be justified, and more detailed drafting advice. The *Guide to Framing Commonwealth Offences* would be an

---

45 Office of Parliamentary Counsel, *OPC Drafting Directions Series* <www.opc.gov.au/about/draft_directions.htm> at 19 November 2009.

46 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].

47 Ibid, [2].

48 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposals 11–7, 12–5.

49 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

appropriate source of guidance for agencies reviewing current secrecy offences or developing new legislative proposals.

11.55 If required, drafting directions issued by the Office of Parliamentary Counsel could draw from this document to provide more detailed directions aimed at technical drafting matters, giving effect to the desired policy framework.

11.56 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.

Recommendation 11–2 The Australian Government Attorney-General's Department should incorporate guidance on the principles contained in Recommendations 8–1 to 8–3, 9–1 to 9–9 and 10–1 to 10–4 in the *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, including:

(a) the circumstances in which the enactment of a specific secrecy offence will be justified; and

(b) the elements of specific secrecy offences, including the requirement that the disclosure cause harm to an essential public interest.

12. Administrative Obligations in the Australian Public Service

Contents

Introduction

12.1 Previous chapters in this Report have considered the regulation of the conduct of Commonwealth officers and others through criminal secrecy offences, including the recommended general secrecy offence and specific secrecy offences. However, the manner in which an individual handles Commonwealth information will also be influenced by a range of administrative and other non-criminal obligations—in

particular, those that apply to Commonwealth employees through the employment relationship. These are the focus of the following three chapters of this Report.

12.2 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 recommendations for clarifying and consolidating these obligations. Procedural safeguards for the investigation and enforcement of administrative secrecy obligations are also discussed.

12.3 Chapter 13 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.

12.4 Chapters 14 and 15 discuss 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.

Background

The Australian Public Service

12.5 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*;[1] and
- statutory agencies, being bodies declared by an Act to be a statutory agency for the purposes of the *Public Service Act*.[2]

---

1 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> at 23 November 2009.

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> at 23 November 2009.

12.6 As at June 2008, more than 160,000 people were engaged as APS employees,[3] with employees and agencies covered by the *Public Service Act* accounting for over two-thirds of the Commonwealth public sector.[4]

Secrecy obligations under the general law

12.7 Aspects of the general law impose duties on employees—including APS employees—not to disclose information in certain circumstances. As discussed in Chapter 3, general law obligations include the equitable doctrine of confidence and employees' common law duty of fidelity and loyalty. These may supplement the statutory secrecy obligations that apply to APS employees, discussed later in this chapter.

12.8 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.[5] 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.[6]

12.9 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'.[7] 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.[8]

12.10 The test for the lawfulness of a direction given to an APS employee is likely to be broader than the common law 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 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

---

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 *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.

6 *R v Darling Island Stevedoring & Lighterage Co Ltd; Ex parte Halliday* (1938) 60 CLR 601, 621–622.

7 *Public Service Act 1999* (Cth) s 13(5).

8 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

Commonwealth as an employer. Also, the direction must be reasonable in all the circumstances.[9]

Secrecy obligations under the *Public Service Act*

Obligations under the APS Code of Conduct

12.11 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, secretaries of departments, heads of executive agencies or statutory agencies, and statutory officeholders.[10] 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;[11]
- maintain appropriate confidentiality about dealings that the employee has with any minister or minister's member of staff;[12] and
- comply with any other conduct requirement that is prescribed in the regulations.[13]

12.12 Regulation 2.1 of the *Public Service Regulations 1999* (Cth)—set out in full in Appendix 5—is the only other conduct requirement prescribed in the regulations. 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.

---

9 Ibid. Where a direction is incompatible with the implied constitutional freedom of political communication, it will not be 'lawful and reasonable': *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334.

10 *Public Service Act 1999* (Cth) ss 7, 14.

11 Ibid s 13(4).

12 Ibid s 13(6).

13 Ibid s 13(13).

12.13 Exceptions to these 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.[14]

12.14 The regulation also expressly preserves an agency head's authority to give 'lawful and reasonable directions' regarding the disclosure of information.[15]

Role of secrecy provisions in the APS Code of Conduct

12.15 In Chapter 4, the ALRC considers the role that administrative secrecy provisions serve in regulating the disclosure of information by Commonwealth officers. First, administrative secrecy obligations may be the only remedy available, or the most appropriate remedy, to address situations where disclosure does not warrant criminal sanctions or criminal sanctions are not available. Secondly, by addressing the distinct context of public sector employment obligations, administrative secrecy provisions also protect different interests from those recognised in the criminal context. In particular, they should 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'.[16]

Consequences of breaching the APS Code of Conduct

12.16 Breach of the APS Code of Conduct gives rise to potential administrative sanctions.[17] However, because of the operation of s 70 of the *Crimes Act 1914* (Cth), an APS employee who breaches the Code's secrecy obligations could also be subject to criminal sanctions.

12.17 As discussed elsewhere in this Report, s 70 of the *Crimes Act* prohibits a person who is, or has been, a Commonwealth officer from disclosing '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'. Regulation 2.1 gives rise to such a duty for the purposes of s 70 and has been used as the basis for prosecutions.[18]

---

14 *Public Service Regulations 1999* (Cth) reg 2.1(5).
15 Ibid reg 2.1(6).
16 *Public Service Act 1999* (Cth) s 3.
17 Ibid s 15.
18 For example, *R v Goreng Goreng* [2008] ACTSC 74.

12.18 In Chapter 4, the ALRC recommends a new general secrecy offence to replace s 70 of the *Crimes Act*. Rather than relying on externally imposed duties, the general secrecy offence expressly targets unauthorised disclosures that are reasonably likely to cause harm to essential public interests. Importantly, in the ALRC's view, a broadly based public interest in the 'effective working of government' is not sufficient to enliven the general offence.

Relationship between secrecy obligations and other APS requirements

12.19 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 to uphold the APS Value of an apolitical public service.[19] 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;[20] and
- behaves at all times in a way that upholds the integrity and good reputation of the APS.[21]

12.20 In Chapter 14, the ALRC discusses the information-handling policies of Australian Government agencies. These policies address a range of issues beyond secrecy. 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 may also include requirements for employees to release information in certain circumstances.[22]

Prejudice to the effective working of government

Background

12.21 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

> 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.[23]

---

19 Attorney-General's Department, *Submission SR 36,* 6 March 2009. See *Public Service Act 1999* (Cth) s 10(1)(a).

20 *Public Service Act 1999* (Cth) s 13(10).

21 Ibid s 13(11).

22 See also Ch 16, which considers the relationship between secrecy laws and other information-handling regimes, such as FOI laws and archives.

23 *Public Service Regulations 1999* (Cth) reg 2.1(3).

12.22 This requirement was introduced in 2006, following the decision of Finn J in *Bennett v President, Human Rights and Equal Opportunity Commission* (*Bennett*)[24] that the broader predecessor of the regulation was inconsistent with the implied constitutional guarantee of freedom of communication about government and political matters.[25]

12.23 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*.[26]

12.24 The scope of the regulation has been further clarified by the Australian Public Service Commission (APSC) in its publication, *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 [*Freedom of Information Act 1982* (Cth) (FOI Act)] are a useful starting point in determining which categories of information may potentially fall within the scope of regulation 2.1.[27]

12.25 The constitutionality of the amended regulation was upheld by Refshauge J of the ACT Supreme Court in *R v Goreng Goreng* (*Goreng Goreng*).[28] He 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.[29] Some concerns remain, however, in relation to the uncertain scope and application of the revised regulation.

12.26 For example, in *Goreng Goreng*, Refshauge J stated that it was with 'considerable hesitation' that he upheld reg 2.1(3) as meeting the requisite standard of

---

24 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334. *Bennett* is considered further in Chs 2, 3.

25 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'.

26 Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006).

27 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009.

28 *R v Goreng Goreng* [2008] ACTSC 74.

29 Ibid, [37].

certainty, on the basis 'that public servants will, by and large, comprehend what is encompassed'.[30] The unclear nature of the obligation was also commented on by Whistleblowers Australia, in its submission in response to the Issues Paper, *Review of Secrecy Laws* (IP 34):

> 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.[31]

12.27 In this Inquiry, the ALRC has considered several options for reforming reg 2.1(3), in order to clarify its scope and application. The ALRC has also considered a potential framework for disciplinary authorities and others to interpret whether particular conduct was in breach of the regulations. These options for reform are considered below.

The 'effective working of government'

12.28 As noted above, reg 2.1(3) is based on the prejudice that a disclosure could cause to the effective working of government. This formulation was largely derived from the comments of Finn J in *Bennett*, where he accepted that secrecy laws designed to meet this end could be compatible with the implied constitutional freedom of communication about government and political matters.[32]

12.29 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 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

30 Ibid, [55].

31 Whistleblowers Australia, *Submission SR 40,* 10 March 2009. Whistleblowers Australia also raised concerns about the use of 'lawful and reasonable directions' by an agency.

32 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334, 358.

(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.[33]

12.30 Another example is found in the *UK Civil Service Management Code*:

> 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.[34]

Submissions and consultations

12.31 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC noted the broad range of situations that may warrant disciplinary action by an Australian Government agency. The ALRC expressed the preliminary view that the requirement of prejudice to the effective working of government was an appropriate way of capturing the many unauthorised disclosures that are legitimately the subject of disciplinary proceedings. Instead, the ALRC focused on narrowing the scope of conduct regulated by amending other aspects of the regulation—for example, by proposing that a disclosure must be 'reasonably likely' to prejudice the effective working of government.[35] The ALRC also developed a framework for interpreting when a disclosure would cause the requisite prejudice.[36]

12.32 The Community and Public Sector Union (CPSU) and Whistleblowers Australia argued against retaining a broad provision based on prejudice to the effective working of government.[37] Whistleblowers Australia expressed the view that:

> There is a difference between reg 2.1 and statutory secrecy provisions which deal with specific, real and factual data. Reg 2.1 is concerned with public service administrative information about some generalised and amorphous matters which lack specificity and are subjectively identified by agencies which have vested interests in the continued secrecy of the information. Conversely other statutory secrecy provisions objectively deal with specific and clearly identified real subjects (e.g. national security, tax or Census records, Customs transactions, Medicare health records or matters directly concerning law enforcement, defence or intelligence information).[38]

12.33 Whistleblowers Australia submitted that so long as 'prejudice to the effective working of government' is retained, any of the ALRC's proposals for reform of

---

33 *Public Sector Management Regulations 1995* (SA) reg 15(d).

34 Minister for the Civil Service (UK), *Civil Service Management Code* <www.civilservice.gov.uk/about/resources/cmsc > at 23 November 2009, [4.2.6].

35 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 13–1.

36 Ibid, Proposal 13–2.

37 Whistleblowers Australia, *Submission SR 74,* 17 August 2009; Community and Public Sector Union, *Submission SR 57,* 7 August 2009; Whistleblowers Australia, *Submission SR 40,* 10 March 2009; Community and Public Sector Union, *Submission SR 32,* 2 March 2009.

38 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.

reg 2.1(3) are merely 'papering over a hole below the waterline'. Whistleblowers Australia commented that such a recommendation would not help APS employees to reach a point of 'clarity, certainty and safety'.[39]

12.34 In its response to IP 34, the Public Interest Advocacy Centre (PIAC) also queried the breadth of a prohibition on the disclosure of information that could prejudice the 'effective working of government':

> 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* working of government') may frequently be in tension with other important public interests, such as the *transparent* working of government.[40]

12.35 In comparison, the Australian Government Attorney-General's Department (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'.[41]

ALRC's views

12.36 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 rely on the fact that these deliberations will be treated confidentially. Members of the public also expect that the information they provide to the APS will be accorded a high level of confidentiality. 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 be protected.

12.37 In the ALRC's view, prejudice to the 'effective working of government' should remain the basis of the administrative secrecy obligation in the APS Code of Conduct because of the broad range of situations where the unauthorised disclosure of information may warrant the imposition of a disciplinary penalty. Attempting to articulate these harms more specifically—as was suggested, for example, by Whistleblowers Australia—risks inappropriately narrowing the provision's scope. This approach should be distinguished from the use of the 'effective working of government' as the basis for criminal sanctions, which the ALRC considers to be overly broad in that context.[42]

---

39 Ibid.
40 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009.
41 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
42 See Chs 4, 5.

12.38 Below, the ALRC makes recommendations to narrow the scope of conduct regulated by reg 2.1(3) of the *Public Service Regulations* to those disclosures that are 'reasonably likely' to prejudice the effective working of government[43] and to clarify the application of the regulation.[44] Further, in Chapter 14, the ALRC recommends that Australian Government agencies should issue information-handling guidelines to help employees and others understand disclosures that are, and are not, the subject of secrecy provisions.[45] These recommendations mitigate the potentially broad scope of 'prejudice to the effective working of government'.

Narrowing the scope of conduct regulated

12.39 In DP 74, the ALRC noted that several of the elements of reg 2.1(3) of the *Public Service Regulations* were different from, and generally broader than, elements of other Commonwealth secrecy provisions. These include:

- the regulation's application to any information that an APS employee obtains or generates *in connection with* his or her employment; and

- breach of the regulation occurring where it is *reasonably foreseeable* that an APS employee's disclosure *could be prejudicial* to the effective working of government.

12.40 These elements are discussed further below, including possible options for reform.

'In connection with'

12.41 Regulation 2.1(3) applies to any information that an APS employee obtains or generates *in connection with* his or her employment. Somewhat narrower constructions have been used in other Commonwealth secrecy provisions. Most commonly, these require that the regulated party has acquired the information 'in the course of', or 'in the performance of', his or her functions or duties.[46] The regulation's application to conduct 'in connection with' the employment of an APS employee is, however, consistent with two other requirements in the APS Code of Conduct:

- the requirement to disclose, and take reasonable steps to avoid, any conflict of interest (real or apparent) in connection with APS employment; and

---

43 Recommendation 12–1.
44 Recommendation 12–2.
45 Recommendation 14–1.
46 The ALRC has identified similar formulations 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.

- the requirement not to provide false or misleading information in response to a request for information that is made for official purposes in connection with the employee's APS employment.[47]

12.42 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(3) or other secrecy provisions. Some limited guidance, however, may be drawn from the interpretation of this phrase in different Commonwealth legislation. For example, the *Administrative Decisions (Judicial Review) Act 1977* (Cth) exempts from the requirement to provide a statement of reasons decisions 'in connection with' the investigation or prosecution of person for a Commonwealth offence.[48] In adjudicating on this exemption, Davies J noted that:

> 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.[49]

12.43 In its good practice guide, *Handling Misconduct*, the APSC explains that 'in connection with' is used to connect a required standard of conduct in the Code and APS employment 'where an employee's actions may have some influence on how they perform their duties'.[50] This can be compared with, for example, 'in the course of employment', which is used 'in direct association with the particular conduct expected of APS employees at work'.[51]

Reasonably foreseeable that disclosure could be prejudicial

12.44 Breach of reg 2.1(3) will occur if it is *reasonably foreseeable* that an APS employee's disclosure *could be prejudicial* to the effective working of government. This sets out an objective test, based on what a reasonable person would decide in the same circumstances and with the same information.[52] In a motion for disallowance of the *Public Service Amendment Regulations 2004* (Cth)—which included an identical provision to the current reg 2.1(3)—Senator Kim Carr commented that:

---

47 *Public Service Act 1999* (Cth) s 13(7), (9).

48 *Administrative Decisions (Judicial Review) Act 1977* (Cth) ss 13(11); sch 2(e)(i).

49 *Hatfield v Health Insurance Commission* (1987) 15 FCR 487, 491. See also *South Pacific Resort Hotels Pty Ltd v Trainor* (2005) 144 FCR 402, where 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 was 'in connection with' the employee's employment for the purpose of s 106 of the *Sex Discrimination Act 1984* (Cth).

50 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), 15.

51 Ibid.

52 Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006), 2.

> '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, because any action 'could be prejudicial' if the political masters of the Public Service deem it to be so.[53]

Submissions and consultations

12.45 In DP 74, the ALRC proposed that reg 2.1 should be amended to apply to information:

- to which an APS employee has access 'by reason of his or her employment' (as compared with information obtained or generated 'in connection with' his or her employment);[54] and

- where the disclosure is 'reasonably likely to prejudice the effective working of government' (as compared with where it is reasonably foreseeable that an APS employee's disclosure could be prejudicial).[55]

12.46 In particular, the ALRC proposed these amendments more narrowly focus the operation of the regulation, which it considered to be particularly important in light of the broad scope of 'prejudice to the effective working of government'. The proposed amendments were also consistent with the proposed elements of the general secrecy offence.

12.47 Civil Liberties Australia supported the proposed amendments. In its view, the threshold for reg 2.1(3) 'has been set far too low' and 'reasonable likelihood' is a more appropriate model to follow.[56] Ron Fraser agreed, noting that the current wording is 'very wide'.[57] A number of Australian Government agencies also supported the proposed amendments to the regulation.[58]

12.48 However, several stakeholders questioned whether it was necessary or desirable to amend reg 2.1(3) as proposed. The APSC expressed the view that amending reg 2.1 to apply to information which is 'reasonably likely to be prejudicial' would 'clearly water down the regulation while … asking individual public servants to make a much more difficult judgement'. The APSC also noted that the use of 'in connection with' had the benefit of capturing situations where an APS employee, for example, browses a

---

53 Commonwealth, *Parliamentary Debates*, Senate, 16 June 2005, 38 (K Carr), 41.

54 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 13–1(a).

55 Ibid, Proposal 13–1(b).

56 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

57 R Fraser, *Submission SR 78,* 21 August 2009.

58 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.

database containing personal information out of interest, rather than accessing it in the performance of his or her official duties.[59]

12.49 The Australian Crime Commission (ACC) also raised concerns about the proposed changes, noting that the disciplinary provisions should remain sufficiently broad in order to 'encompass a range of minor wrongdoings that merits some indication of disapproval'.[60] The Australian Privacy Foundation was concerned that the proposed amendments would excuse APS employees from any consequences relating to unauthorised disclosures that breach personal privacy, but are not considered to be prejudicial to the workings of government.[61]

12.50 For others, however, the proposed changes did not go far enough. For example, although Whistleblowers Australia supported the 'reasonably likely' to cause harm threshold, it suggested that this benefit was largely undone by the retention of the 'prejudice to the effective working of government' requirement.[62] The CPSU suggested that the 'minor amendments' proposed by the ALRC would not fix the broad scope and uncertainty of reg 2.1(3). It argued that even with this narrowing, the provision could still operate as a 'catch-all provision of uncertain scope and indeterminate application', remaining 'an effective way of fostering a culture of secrecy in the public service and unnecessarily inhibiting openness and accountability of government'.[63]

12.51 In comparison, in the view of the Australian Taxation Office (ATO), the proposed reforms would not significantly change the outcome of determinations under reg 2.1(3).[64]

ALRC's views

12.52 As indicated above, the ALRC accepts that prejudice to the effective working of government is a suitable statement of harm in the context of administrative disciplinary sanctions, given the need to encompass a wide variety of situations where an APS employee who discloses Commonwealth information without authorisation could appropriately be subject to disciplinary penalties. However, given the broad nature of the identified harm, a rigorous threshold is important to forestall the potentially indiscriminate application of the provision. In particular, the ALRC is concerned about the potential breadth of the application of the regulation to disclosures where it is *reasonably foreseeable* that prejudice *could* result to the effective working of government. The ALRC concludes, therefore, that the appropriate balance is achieved

---

59 Australian Public Service Commission, *Submission SR 56,* 7 August 2009. The APS gave the further example of an APS employee who 'talked shop' with another employee outside his or her work area and revealed information that he or she had a duty not to disclose.

60 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

61 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

62 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.

63 Community and Public Sector Union, *Submission SR 57,* 7 August 2009.

64 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

by limiting the regulation to apply to disclosures that are 'reasonably likely' to be prejudicial to the effective working of government.

12.53 In making this recommendation, the ALRC took into account the potential detriment of an APS employee *not* sharing information in some situations. Disclosing information is a core aspect of an open and accountable system of government—one of the factors to which the ALRC is directed to have regard in this Inquiry.[65] An important part of facilitating a culture of open government in Australian Government agencies is ensuring that APS employees have confidence to disclose information in appropriate circumstances. Where a disclosure has no reasonable likelihood of prejudicing any aspect of the effective working of government, an APS employee should not be subject to sanctions (including disciplinary sanctions) for releasing the information.

12.54 Some stakeholders were concerned that a test of 'reasonably likely to be prejudicial' would be too narrow to adequately cover the range of disclosures warranting disciplinary action. In the ALRC's view, this concern is largely dispelled by the manner in which courts have interpreted what is necessary to establish a 'reasonable likelihood'. For example, in *Department of Agriculture and Rural Affairs v Binnie*, the Supreme Court of Victoria interpreted 'reasonably likely to endanger' a person's life or physical safety in the context of the *Freedom of Information Act 1982* (Vic). The Court agreed that 'reasonably likely' had a different connotation from 'likely' on its own. Rather, as stated by Marks J, the expression

> speaks of a chance of an event occurring or not occurring which is real—not fanciful or remote. It does not refer to a chance which is more likely than not to occur, that is, one which is 'odds on', or where between nil and certainty it should be placed. A chance which in common parlance is described as 'reasonable' is one that is 'fair', 'sufficient' or 'worth noting'.[66]

12.55 This case concerned the Victorian freedom of information legislation. Because the interpretation of 'reasonably likely' may vary depending on the context of the legislation, the courts may adopt a slightly different test where the phrase is used to support administrative disciplinary proceedings.[67] However, this line of reasoning strongly indicates that the revised regulation would not require a disciplinary authority to conclusively establish that prejudice from an unauthorised disclosure is more likely than not to occur.

12.56 The ALRC also recognises that disclosures that do not meet the higher threshold recommended for reg 2.1(3) may still be the subject of disciplinary proceedings on the basis of other requirements of the APS Code of Conduct, such as the obligation to

---

65 The Terms of Reference are set out at the front of this Report. Open government principles are discussed in Ch 2.

66 *Department of Agriculture and Rural Affairs v Binnie* [1989] VR 836, 842.

67 See, eg, discussion in Ibid, 840–841 for the different application of 'reasonably likely' in the context of criminal offences.

'behave with honesty and integrity in the course of APS employment' and 'comply with all applicable Australian laws'. This would include, for example, compliance with relevant privacy laws.

12.57 Another concern that was raised was that a test of 'reasonable likelihood' would be a more difficult judgment for APS employees than the current test—that is, whether it is reasonably foreseeable that prejudice could result to the effective working of government. The ALRC does not consider this to be a valid reason for retaining an unduly broad secrecy provision. In Chapters 14 and 15 the ALRC makes a number of recommendations directed towards assisting APS employees and others to understand and comply with their information-handling responsibilities. These include, for example, that Australian Government agencies should develop and implement information-handling policies and guidelines clarifying the application of relevant secrecy laws to their information holdings[68] and providing avenues for employees to raise queries or concerns.[69] In the ALRC's view, these strategies adequately address the potential difficulty that an APS employee may face in deciding whether the disclosure of information would be 'reasonably likely' to prejudice the effective working of government.

12.58 In the ALRC's view, the application of reg 2.1(3) to information that an APS employee obtains or generates 'in connection with' his or her employment is appropriate. This terminology is consistent with other conduct requirements in the APS Code of Conduct. There is not a sufficient difference between the likely application of 'in connection with' and the term proposed in DP 74 'by reason of his or her employment', to warrant reform. In particular, the general words 'in connection with' will be confined by the context of the regulation—namely, an 'APS employee's employment'.[70]

Recommendation 12–1 Regulation 2.1(3) of the *Public Service Regulations 1999* (Cth) should be amended to apply to information where the disclosure is reasonably likely to prejudice the effective working of government.

Developing an interpretive framework

12.59 In DP 74, the ALRC noted stakeholder concerns that there was insufficient guidance available to APS employees on what disclosures would breach reg 2.1(3). The ALRC suggested that the regulation's application could be clarified by establishing a framework for disciplinary authorities to use when determining whether particular conduct amounted to a breach. In particular, the ALRC proposed that disciplinary authorities should have regard to:

68 Recommendation 14–1.
69 Recommendation 15–3.
70 D Pearce and R Geddes, *Statutory Interpretation in Australia* (5th ed, 2001), [4.18].

(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.[71]

12.60 The interpretive framework was designed to facilitate a complementary approach to secrecy and the *Freedom of Information Act 1982* (Cth) (FOI Act) in an agency's information-handling regime. The ALRC noted that the Australian Parliament has indicated in the FOI Act the types of information that warrant a heightened level of protection by specifying which documents may be denied access to by an agency. Both the Explanatory Statement for reg 2.1 and the *APS Values and Code of Conduct in Practice* make clear that the availability of these exemptions may indicate the potential for a disclosure to prejudice the effective working of government.

12.61 The ALRC acknowledged, however, that 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. The circumstances of disclosure may be as, or more, important than the information itself. Accordingly, the proposed framework included consideration of whether an APS employee took reasonable steps to comply with the agency's information-handling policy or a lawful and reasonable direction regarding the disclosure of information.

Submissions and consultations

12.62 A number of Australian Government agencies and other stakeholders supported the development of a framework for interpreting whether a disclosure was reasonably likely to harm the effective working of government.[72]

12.63 However, several stakeholders were concerned that the proposed interpretive framework could require APS employees to become familiar with the complexities of FOI law.[73] The APSC, for example, was concerned that an interpretive framework 'would, in effect, read into the new regulation all of the exemptions and subtleties that relate to the release of material under the FOI Act'. This would be difficult for APS

---

71 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 13–2.

72 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

73 Australian Public Service Commission, *Submission SR 56,* 7 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

employees to consider 'on the ground'. In the APSC's view, its use would be more appropriate from a practitioner's or investigator's perspective.[74]

12.64 The CPSU also suggested that the proposal should incorporate clear exceptions to the application of reg 2.1, for example:

> where the disclosure of information causes embarrassment rather than harm to the government, generates legitimate political communication about matters of public interest or is trivial and inconsequential.[75]

ALRC's views

12.65 Throughout the course of this Inquiry, serious concerns have been expressed about the uncertain scope of reg 2.1(3). Clear criteria for assessing whether a disclosure was reasonably likely to cause harm to the effective working of government would go a long way towards addressing these concerns.

12.66 Broadly speaking, the disclosure of information by an APS employee could prejudice the effective working of government in two ways—by the *nature* of the information disclosed; or by the c*ircumstances* of the disclosure. The respective importance of these factors will be governed by the context of the disclosure. Where, for example, particularly sensitive information is disclosed, the dominant concern is the nature of the information. In other situations, an APS employee might, for example, make multiple disclosures of somewhat less sensitive information, each time breaching agency policies and guidelines. Here, the dominant concern is the circumstances of the disclosure.

12.67 The *APS Values and Code of Conduct in Practice* already advises that the exemptions set out in the FOI Act are 'a useful starting point' in determining whether a disclosure falls within the scope of reg 2.1. This guidance should be extended to outline other situations that may indicate that a disclosure of information is reasonably likely to prejudice the effective working of government. In particular, this would include where prejudice results from the circumstances of a particular disclosure, or series of disclosures—for example, the consistent failure by an APS employee to follow an agency's policy for the release of information.

12.68 The ALRC agrees with the CPSU that it would be beneficial to identify situations where the effective working of government would *not* be prejudiced. This could include, for example, where the only prejudice that may result from the disclosure of information is embarrassment to the government, or where the disclosure is trivial and inconsequential. A clear statement that a disclosure that is merely embarrassing to the government does not constitute the requisite prejudice is consistent

74 Australian Public Service Commission, *Submission SR 56,* 7 August 2009.
75 Community and Public Sector Union, *Submission SR 57,* 7 August 2009.

with the operation of the FOI Act[76] as well as limitations that have been placed on the application of the equitable doctrine of breach of confidence to government information.[77]

Recommendation 12–2 The Australian Public Service Commission should amend the *APS Values and Code of Conduct in Practice* to provide further guidance on what is meant by 'reasonably likely to prejudice the effective working of government' in reg 2.1 of the *Public Service Regulations 1999* (Cth), as revised in Recommendation 12–1. This should include:

(a) that prejudice may arise from the nature of the information disclosed, such as where the information would not be subject to release under the *Freedom of Information Act 1982* (Cth) or through some other means;

(b) that prejudice may arise from the circumstances in which the disclosure is made, such as where an Australian Public Service employee did not take reasonable steps to comply with the agency's information-handling policy or any lawful and reasonable direction concerning the disclosure of information; and

(c) the fact that a disclosure could, for example, result in embarrassment to the government is not sufficient to establish prejudice.

Information communicated in confidence

Background

12.69 Regulation 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.[78]

---

76 See, eg, Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [1.6.3.2.4]. Under the Exposure Draft, Freedom of Information Reform Bill 2009 (Cth), the fact that access to a document could 'result in embarrassment to the Commonwealth Government' is an irrelevant factor in assessing the public interest in disclosing information. Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) cl 11B.

77 *Commonwealth v Fairfax* (1980) 147 CLR 39. The equitable doctrine of breach of confidence, including its application to government information, is discussed in Ch 3.

78 *Public Service Regulations 1999* (Cth) reg 2.1(4).

12.70 The Explanatory Statement for the 2006 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).[79]

12.71 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.[80]

12.72 In DP 74, the ALRC noted the substantial overlap between reg 2.1(4)—information communicated in confidence—and the ALRC's proposed revisions to reg 2.1(3)—information which, if disclosed, would be prejudicial to the effective working of government either on the basis of the nature of the information or the circumstances of its disclosure.

12.73 One indication that the disclosure of information could prejudice the effective working of government on the basis of the nature of the information is the availability of an exemption under the FOI Act. Several FOI exemptions are relevant to confidential information. First, an exemption applies where the disclosure of a document under the FOI Act 'would found an action, by a person (other than an agency or the Commonwealth), for breach of confidence'.[81] A further exemption applies 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.[82]

---

79 Explanatory Statement, *Public Service Amendment Regulations (No 1) 2006* (Cth) (SLO No 183 of 2006), 3.

80 Ibid.

81 *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 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) does not amend this exemption.

82 *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 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) does not amend these exemptions.

12.74 The disclosure of confidential information by an APS employee could also prejudice the effective working of government on the basis of the circumstances of the disclosure. This is likely to be the case, for example, in relation to the disclosure of security classified information.[83]

12.75 As discussed in Chapter 3, 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'.[84] In *Commonwealth v Fairfax*, the High Court discussed how this principle could apply to government information. The Court held that, beyond simply demonstrating the confidential nature of the information, the government must show that it would be to its detriment for the information to be communicated. The claim to confidentiality will be determined 'by reference to the public interest'—only those disclosures that are likely to injure the public interest will be protected.[85]

Submissions and consultations

12.76 In DP 74, the ALRC proposed that the express prohibition on the disclosure of information communicated in confidence set out in reg 2.1(4) should be removed.[86] This was supported by a number of government and other stakeholders.[87]

12.77 However, several Australian Government agencies were strongly of the view that a separate provision for the protection of confidential information should be retained[88]—even where they acknowledged that such disclosures were likely to fall within the scope of 'prejudice to the effective working of government'.[89] The ACC, for example, submitted that a provision that clearly applied to confidential information provided stronger protection for information that is provided in confidence to it for the national criminal intelligence database. This was considered preferable to relying on 'implications drawn from a broad provision about the effective working of government'.[90] This position was consistent with advice from the APSC that, in developing reg 2.1, some agencies were keen to ensure that *all* confidential information was explicitly covered by the regulation.[91]

---

83 The security classification system for the Australian Government is discussed in Ch 14.
84 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50, citing *Lord Ashburton v Pope* (1913) 2 Ch 469, 475.
85 *Commonwealth v Fairfax* (1980) 147 CLR 39, 52.
86 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 13–3.
87 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
88 See, eg, Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.
89 See, eg, Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.
90 Australian Crime Commission, *Submission SR 75,* 19 August 2009.
91 Australian Public Service Commission, *Submission SR 56,* 7 August 2009.

ALRC's views

12.78 Where there is no reasonable likelihood that disclosure would result in prejudice to the effective working of government, the ALRC is not convinced that there is a valid public policy basis for exposing an APS employee to disciplinary action. Consistently with this 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.

12.79 This recommendation recognises the important balance between the public interests in protecting certain information from disclosure, as against the public interests in facilitating open and accountable government. The recommendation also accords with limitations that have been placed on the protection of confidential information held by government pursuant to the equitable doctrine.[92]

12.80 In other parts of this Report, the ALRC has considered the protection of confidential information held by the Australian Government through the operation of criminal sanctions. Generally, the ALRC has expressed the view that a Commonwealth officer should only be subject to criminal proceedings for disclosing confidential information where the particular disclosure caused, or was reasonably likely, or intended to cause, harm to an essential public interest[93]—for example, damage to the flow of information between governments and international organisations.[94]

12.81 In Chapter 8, the ALRC accepts that a tightly defined subset of confidential information may be given protection as a category of information under criminal secrecy offences, without the need to prove that the disclosure of that information caused, or was likely or intended to cause, harm.[95] An APS employee who discloses confidential information in breach of any such offence may be subject to administrative proceedings through s 13(4) of the *Public Service Act*.[96]

Recommendation 12–3 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.

92 *Commonwealth v Fairfax* (1980) 147 CLR 39.
93 The term 'essential public interest' is defined in Ch 1.
94 See Ch 5.
95 Recommendation 8–2.
96 As noted above, *Public Service Act 1999* (Cth) s 13(4) requires an APS employee, when acting in the course of APS employment, to comply with all applicable Australian laws.

Exceptions and defences

Background

12.82 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.[97]

12.83 It is notable that 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*:

> 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.[98]

12.84 The relationship between public interest disclosures under 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.*[99]

---

97 *Public Service Regulations 1999* (Cth) reg 2.1(5).

98 *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.

99 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009, 103.

12.85 Where an APS employee discloses information within the parameters of s 16 of the *Public Service Act*, such a report would attract the exceptions in reg 2.1(5) for information disclosed 'in the course of the APS employee's duties' or 'otherwise authorised by law'. Accordingly, he or she would not be liable to disciplinary action.

12.86 The scope of protection, however, is not comprehensive. In particular, a disclosure will only be protected 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.[100] 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 reporting disclosures and recommended that bodies authorised to receive and investigate public interest disclosures should also include the Commonwealth Ombudsman and integrity agencies.[101]

12.87 In its submission in response to 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.[102]

Submissions and consultations

12.88 In DP 74, the ALRC proposed that reg 2.1 should include a note cross-referencing to the immunity provided by proposed Commonwealth public interest disclosure legislation. Those stakeholders that commented on this issue unanimously supported the proposal.[103]

---

100 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.

101 Ibid, Ch 7, Recs 17, 18.

102 Community and Public Sector Union, *Submission SR 32,* 2 March 2009.

103 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009.

12.89 Whistleblowers Australia reiterated its concerns about the operation of s 16 of the *Public Service Act*, a provision it considered to be 'impotent and ineffective' in protecting APS employees who 'make a well-intentioned disclosure that they believe would serve the public interest'. It argued that 'the only redeeming feature of [the] scheme' was that 'it is so patently unworkable that few officers put themselves at risk by using it'.[104] It recommended that s 16 be repealed upon the introduction of Commonwealth public interest disclosure legislation.[105]

12.90 Whistleblowers Australia also queried the exception in reg 2.1(5)(d)(i) for information which 'is already in the public domain as a result of a disclosure of information that is lawful under these regulations or another law'. This exception, it said, 'implies the obvious': if information has been lawfully disclosed once then it is not a new offence to disclose it a second time.[106]

ALRC's views

12.91 The ALRC considers that robust public interest disclosure legislation is an essential corollary of Commonwealth secrecy obligations, including administrative obligations in the *Public Service Act*. The limited scope of s 16 of the *Public Service Act* prevents it from adequately performing this function.

12.92 As discussed in Chapter 2, the ALRC is assuming in this Report 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. The proposed legislation would provide immunity from liability under reg 2.1 for disclosures made within the public interest disclosure framework.

12.93 The ALRC has decided not to recommend that secrecy provisions in Commonwealth legislation should include notes expressly cross-referring to the immunity provided by Commonwealth public interest disclosure legislation. For the reasons set out in Chapter 7, such a note is considered unnecessary. APS employees must, however, be clearly informed about the availability of public interest disclosure mechanisms in other ways. In particular, in Chapter 14 the ALRC recommends that Australian Government agencies should develop and implement policies clarifying the application of relevant secrecy laws to their information holdings. These should include avenues for an employee to raise queries or concerns, including the process by which he or she can make a public interest disclosure.[107]

12.94 Other than Whistleblowers Australia's concerns about the exception for publicly available information, which is dealt with below, the ALRC has not been made aware

104 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.
105 Ibid.
106 Ibid.
107 Recommendation 14–1.

of any issues with the exceptions currently set out in reg 2.1. These exceptions provide important limitations on 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 recommended general secrecy offence.[108]

12.95 The exception in reg 2.1(5)(d)(i) for information that is already in the public domain as a result of a lawful disclosure serves a useful role in administrative secrecy regimes. To illustrate, the media could report an anonymous leak of budget information before the budget's public release. It is reasonably likely that an APS employee who confirms the leak, and consequently validates the information, could cause prejudice to the effective working of government. However, once information is lawfully available, then no prejudice to the effective working of government could result from its disclosure, regardless of the circumstances of its disclosure.

Penalties

Background

12.96 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;[109] and a reprimand.[110] An agency head may also prescribe other action in order to reduce the risk of further misconduct provided it is clearly cast as management action and not a penalty.[111]

12.97 Within these parameters, each agency head can decide whether to impose an administrative penalty for a breach of the Code of Conduct, and what type of administrative penalty to impose. 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

---

108 See Ch 7.

109 *Public Service Act 1999* (Cth) s 15; *Public Service Regulations 1999* (Cth) reg 2.3. The House of Representatives Standing Committee on Legal and Constitutional Affairs 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': 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.

110 *Public Service Act 1999* (Cth) s 15.

111 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 could involve, for example, restricting an employee's access to certain information.

> 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.[112]

12.98 In *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'.[113] Sanctions for breach, therefore, 'should focus on reducing or eliminating the likelihood of future similar behaviour'.[114] The APSC goes on to advise that:

> 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.[115]

12.99 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.[116] 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.[117]

Submissions and consultations

12.100 In IP 34, the ALRC asked whether the range and level of administrative penalties available for breaches of secrecy provisions committed by Commonwealth

---

112 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.

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.

114 Ibid.

115 Ibid, 56.

116 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.

117 Ibid, 62.

officers were adequate and appropriate.[118] The ALRC also questioned whether administrative penalties for breach of similar types of secrecy provisions were being applied consistently across Australian Government agencies.[119]

12.101 Only a small number of stakeholders made submissions on these questions.[120] 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.[121] Whistleblowers Australia and Liberty Victoria suggested that any penalties should be commensurate with the potential harm that could result from the disclosure.[122] The Department of Human Services added that penalties 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.[123]

12.102 The ALRC did not propose any reform of the range of administrative penalties for breach of secrecy provisions in DP 74. Instead, the ALRC focused on clarifying the manner in which an agency will apply administrative penalties for breaches of such provisions. In particular, the ALRC proposed that agency information-handling policies 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.[124]

12.103 Most stakeholders that commented on this issue agreed with the ALRC's proposed approach.[125] The ATO advised that it already provides its employees with information about their secrecy obligations and the consequences of breaching those obligations. The ACC noted the potential usefulness of the proposed guidance but questioned why this sort of detail should be required in relation to disclosure of information as opposed to other misconduct issues. It also commented on the importance of ensuring that any attempt to identify relevant factors did not result in decision makers getting the impression that the listed factors were the only ones they

---

118 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 5–12.

119 Ibid, Question 5–15.

120 See, eg, 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.

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

122 Whistleblowers Australia, *Submission SR 40,* 10 March 2009; Liberty Victoria, *Submission SR 19,* 18 February 2009.

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

124 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 13–5.

125 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

needed to take into account. This could result in errors of law in making particular decisions.[126]

ALRC's views

12.104 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. Accordingly, the ALRC does not recommend reform of the range of administrative penalties for breach of secrecy provisions.[127]

12.105 However, there is scope for clarifying the manner in which an agency will apply administrative penalties for breaches of secrecy provisions. In Chapter 14, the ALRC recommends that Australian Government agencies should develop and implement policies and guidelines clarifying the application of relevant secrecy laws to their information holdings.[128] These policies should advise APS employees about the administrative penalties that could result from breach of a secrecy obligation, including 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.

12.106 The above factors are an inclusive, rather than an exhaustive, list of the considerations that a decision maker should take into account in determining the appropriate sanction. They are intended to give employees an idea of the likely implications of breach of a secrecy provision. A publicly available policy might also assist an APS employee who has been sanctioned for such a breach to assess whether he or she should appeal the severity of the sanction—for example, to the Merit Protection Commissioner.

Recommendation 12–4 The information-handling policies developed by Australian Government agencies in accordance with Recommendation 14–1 should set out the disciplinary penalties that may result from breach of secrecy obligations and an inclusive list of the factors that will be considered in determining a penalty.

126 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

127 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.

128 Recommendation 14–1.

Processes for dealing with breaches

12.107 Previous sections of this chapter have addressed the administrative secrecy obligations that should be imposed on APS employees. The following, and final, section discusses the processes that Australian Government agencies should use to determine whether a breach has occurred. First, it assesses the procedural requirements for determining misconduct required by the *Public Service Act*. Secondly, it considers issues that arise in relation to concurrent administrative and criminal proceedings for alleged breaches, including recommendations for reform.

Processes set out in the *Public Service Act*

Determining whether the Code of Conduct has been breached

12.108 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.[129]

12.109 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;[130]
- the process for determining whether an APS employee has breached the Code of Conduct to be carried out informally and expeditiously;[131]
- 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;[132] and
- a written record to be prepared noting the outcome of the investigation.[133]

---

129 *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.
130 *Public Service Commissioner's Directions 1999* (Cth) cl 5.2.
131 Ibid cl 5.3.
132 Ibid cl 5.4.
133 Ibid cl 5.5.

12.110 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. Rather, the steps that will satisfy procedural fairness obligations will depend on the circumstances of each case.[134]

Suspension of employment and reassignment of duties

12.111 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.[135]

12.112 Suspension is subject to a number of conditions, and may be with or without remuneration.[136] Other than in exceptional circumstances, suspension without remuneration is to be for no longer than 30 days.[137] The agency head must review the suspension at reasonable intervals,[138] and the suspension must be ended 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 warranted.[139] Finally, 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.[140]

12.113 An agency head is normally required to exercise his or her powers of suspension having 'due regard for procedural fairness'.[141] This requirement need not apply where the agency head is satisfied, on reasonable grounds, that it would not be appropriate in the circumstances.[142] 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.[143]

---

134 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

135 *Public Service Regulations 1999* (Cth) reg 3.10.

136 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.

137 *Public Service Regulations 1999* (Cth) reg 3.10(3).

138 Ibid reg 3.10(4).

139 Ibid reg 3.10(5).

140 Ibid reg 3.10(6).

141 Ibid reg 3.10(7).

142 Ibid.

143 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

12.114 As an alternative to suspension, an agency head may temporarily re-assign an employee's duties while the employee is investigated for a suspected breach of the Code of Conduct.[144]

Review of findings of breach

12.115 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).[145] Where a person's employment has been terminated, the employee may seek redress under the *Fair Work Act 2009* (Cth). Employees also have the right to seek judicial review by the Federal Court of the agency-level decision.[146]

12.116 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?[147]

12.117 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.[148] If the MPC is not satisfied with the response by the agency head, the MPC may report the matter to the relevant minister, the Prime Minister or Parliament.[149] In 2008–09, the MPC reported that all but two of the recommendations made in relation to applications for review of action were accepted by the agency concerned.[150]

12.118 The importance of checks and balances in disciplinary proceedings, including APS employees having access to review of employment actions for alleged breaches of the APS Code of Conduct, was highlighted in the matter of *Trent Latham*

---

144 *Public Service Act 1999* (Cth) s 25.

145 *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).

146 *Administrative Decisions (Judicial Review) Act 1977* (Cth); *Judiciary Act 1903* (Cth) s 39B.

147 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.

148 *Public Service Regulations 1999* (Cth) reg 5.32.

149 *Public Service Act 1999* (Cth) s 33(6).

150 Australian Public Service Commissioner, *Annual Report 2008–09* (2009), 95–96.

Smith v Department of Foreign Affairs and Trade,[151] (*Trent Latham Smith*) set out in the case study below.

Case study: *Trent Latham Smith v Department of Foreign Affairs and Trade*

Mr Trent Latham Smith brought an action in the Australian Industrial Relations Committee after his employment was terminated by the Department of Foreign Affairs and Trade (DFAT). One aspect of the disciplinary proceeding concerned an email that Mr Smith sent to an adviser for Kevin Rudd (then the Opposition spokesperson on Foreign Affairs) referring the adviser to information in publicly available sources, including *Hansard*.

Since the email did not contain any sensitive or classified information, DFAT did not base its determination on breach of reg 2.1 of the *Public Service Regulations*. Instead, it contended that Mr Smith had suggested to the Opposition a line of questioning that might embarrass the Government. DFAT determined that this was in breach of his obligation to perform his duties in an 'apolitical' manner.[152]

Commissioner Deegan dismissed this reasoning as drawing 'an incredibly long bow'. Mr Smith could not have known that the Opposition's merely asking a question about the information provided could cause some embarrassment. Commissioner Deegan also raised serious concerns about DFAT's process in making a determination of breach, including long delays in the collection of evidence and asking officers to comment on incomplete, and even unseen, evidence.

The termination of Mr Smith was held to be harsh, unjust and unreasonable, and, accordingly, DFAT was ordered to reinstate his employment.

An obligation to report misconduct?

12.119 Some public servants working in the law enforcement context are under an express obligation to report disciplinary breaches and misconduct of which they are aware. For example, the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity has noted that AFP employees are under an obligation to report all contraventions of the professional standards.[153] That committee has recommended that:

> The Australian Government review existing obligations on employees of Commonwealth law enforcement agencies to report misconduct. The review should consider whether these arrangements need to be strengthened, including by legislative

151 *Trent Latham Smith v Department of Foreign Affairs and Trade* [2007] AIRC 765.
152 *Public Service Act 1999* (Cth) s 13(11), applying *Public Service Act 1999* (Cth) s 10(1)(a).
153 Parliament of Australia—Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity, *Inquiry into Law Enforcement Integrity Models* (2009), [5.46].

> means, and whether there are sufficient measures in place to support and protect whistleblowers.[154]

12.120 No express reporting requirement applies to APS employees. However, the APSC good practice guide, *Handling Misconduct*, provides that some APS employees may be obliged to report misconduct in order to comply with requirements of the APS Values and Code of Conduct[155] and the *Public Service Commissioner's Directions*.[156] These include, for example, that an APS employee must 'model and promote' the highest standard of ethical behaviour, taking into account his or her duties and responsibilities:[157]

> As such, the Commission considers that the duty to act with integrity and with the highest ethical standards imposes a reporting obligation on all employees with regard to suspected misconduct. In some circumstances, particularly for employees with managerial responsibilities, it could be a breach of the Code for an employee not to report suspected misconduct.[158]

Submissions and consultations

12.121 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.[159]

12.122 Only a few stakeholders responded to this issue.[160] The AGD supported the existing procedural requirements in the *Public Service Act*, advising that these provide a useful mechanism to deal with minor breaches.[161] The Australian Press Council suggested that, before a 'severe administrative penalty' is imposed on a Commonwealth officer, he or she should have the opportunity to have the case heard by a court or tribunal that can adjudicate on questions of public interest and intent, as well as make findings of fact.[162]

12.123 In DP 74, the ALRC did not make any proposals to reform the processes for determining breaches of administrative secrecy provisions.[163]

---

154 Ibid, Rec 7.
155 *Public Service Act 1999* (Cth) ss 10 and 13, respectively.
156 *Public Service Commissioner's Directions 1999* (Cth). See discussion 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), 25–26.
157 *Public Service Commissioner's Directions 1999* (Cth) dir 2.5(2).
158 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), 26.
159 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–5.
160 See, eg, Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009; Australian Press Council, *Submission SR 16,* 18 February 2009.
161 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
162 Australian Press Council, *Submission SR 16,* 18 February 2009.
163 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), [13.135].

ALRC's views

12.124 Stakeholders in this Inquiry have not raised 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 recommending reforms to these requirements.

12.125 However, the ALRC recognises the imperative for administrative secrecy provisions to be applied in accordance with just and effective disciplinary processes. Cases such as *Trent Latham Smith* illustrate the potential for internal processes to fall short of the requirements of procedural fairness. In particular, the ALRC notes the importance of review mechanisms and oversight bodies in ensuring that agencies handle their disciplinary obligations responsibly. The role of oversight bodies, including the proposed Information Commissioner, is discussed further in Chapter 15.

12.126 Disciplinary processes should also operate alongside readily available avenues for APS employees to raise concerns and complaints, as an aspect of maintaining the effective working of government. As noted above, the introduction of robust whistleblower protections is a fundamental premise of the recommendations in this Report. This is especially important in situations where APS employees are encouraged—or even under an obligation—to report misconduct.

Concurrent administrative and criminal proceedings

12.127 An APS employee suspected of breaching a secrecy law may be subject not only to administrative, but also criminal, proceedings.[164] This raises issues as to the appropriate pathway to pursue, and the order in which proceedings should occur, including implications of this decision for the APS employee in relation to any evidence that he or she gives.

12.128 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.[165]

---

164 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.

165 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

12.129 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.[166]

12.130 What is the position of an APS employee facing both administrative and criminal proceedings? For example, how is an APS employee to participate fully in the administrative proceedings while seeking to exercise his or her right to silence or privilege against self-incrimination in a pending criminal prosecution? 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 right to silence or the privilege against self-incrimination) does not prevent a misconduct process from proceeding.[167]

12.131 In *Goreng Goreng v Jennaway*,[168] the Federal Court considered whether an agency should postpone its review of Ms Goreng Goreng's suspension—an administrative disciplinary action in connection with an investigation of her alleged breach of reg 2.1. The applicant argued that, as she was choosing to exercise her right to 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'.[169] However, this did not 'ordain the postponement, perhaps for an indefinite period, of an administrative process'.[170] In the absence of any legislative provisions to the contrary, Flick J held that whether administrative processes were postponed pending the resolution of criminal proceedings was a discretionary matter for the agency.

12.132 A similar issue was before the Federal Court in *Baker v Commissioner of Federal Police*, in which members of the AFP who were facing criminal charges relating to alleged assaults sought to stay the decision by the AFP whether to terminate their employment pending determination of the criminal proceedings.[171] Gyles J

---

166 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.

167 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

168 *Goreng Goreng v Jennaway* (2007) 164 FCR 567.

169 Ibid, [48].

170 Ibid, [48]–[50].

171 *Baker v Commissioner of Australian Federal Police* (2000) 104 FCR 359.

followed the 'long line of authority' stemming from *McMahon v Gould*,[172] which established that the granting of a stay of civil proceedings is discretionary in the civil court, and the choice of either fully pursuing a civil claim or not doing so to avoid the risk of self-incrimination is not sufficient, in itself, to warrant a stay. Despite dismissing the application, Gyles J agreed that there is 'some merit' in the submission that the manner in which this authority is now applied should be reconsidered to determine whether too little weight is given to the practical as well as legal prejudice to the accused.[173]

12.133 Below, the ALRC canvasses two options for reform to address the threat of 'real prejudice or injustice' arising from concurrent administrative and criminal proceedings: first, a mandatory stay of disciplinary proceedings and, secondly, a 'use immunity' for evidence adduced in such a proceeding.

Mandatory stay of proceedings

12.134 One option for preventing the difficulties that arise with concurrent proceedings is to impose a mandatory stay of disciplinary proceedings on the commencement of criminal proceedings for the same, or substantially the same, conduct. This option would be consistent with the approach recommended by the ALRC in its 2002 report, *Principled Regulation* (ALRC 95), in the context of concurrent civil and criminal proceedings.[174] A mandatory stay of proceedings where concurrent criminal proceedings are commenced has also been included in a number of civil penalty provisions.[175]

12.135 However, it can be argued that the objects of administrative disciplinary proceedings raise different considerations from civil penalty proceedings as considered in ALRC 95. A key basis for the ALRC's recommendation was 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 proceedings … 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

172 *McMahon v Gould* (1982) 7 ACLR 202.

173 *Baker v Commissioner of Australian Federal Police* (2000) 104 FCR 359, 366.

174 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 11–2. The ALRC further recommended that: no, or no further, civil penalty proceedings may be taken against a person if that person has been convicted of that criminal offence. Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002).

175 For example, *Fair Work Act 2009* (Cth) s 553; *National Greenhouse and Energy Reporting Act 2007* (Cth) s 36; *Water Act 2007* (Cth) s 154; *Corporations Act 2001* (Cth) s 1317Q; *Broadcasting Services Act 1992* (Cth) s 205M.

> least to some extent, punitive in nature, double jeopardy protection should be extended to subsequent civil penalty proceedings for the same conduct.[176]

12.136 In comparison, 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' in that service.[177] 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.[178]

Limitations on the admissibility of evidence

12.137 Imposing limitations on the admissibility in criminal proceedings of evidence adduced in disciplinary proceedings is another possible strategy. Any statutory limitation in this regard would supplement general rules and procedures that limit the use of admissions in criminal proceedings. These rules and procedures include the test of 'voluntariness' (the common law admissibility requirement for admissions) and the discretion to exclude admissions where, having regard to the circumstances in which the admission was made, it would be unfair to the defendant to use the evidence.[179]

12.138 In ALRC 95, the ALRC recommended that—in addition to a mandatory stay of proceedings—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. This recommendation responded to concerns that the use of evidence in more than one proceeding could blur important distinctions between the criminal and civil process, including the difference between the criminal and civil standards of proof.[180]

12.139 The ALRC was also concerned that evidence collected in a civil penalty proceeding is not subject to the same procedural protections as those that apply in criminal investigations and prosecutions. Accordingly, 'to allow evidence given in civil

---

176 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), [11.37].

177 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.

178 *Pillai v Messiter [No 2]* (1989) 16 NSWLR 197, 201.

179 *Evidence Act 1995* (Cth) s 90. These tests are discussed in Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), Ch 10.

180 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 11–3 and surrounding text.

penalty proceedings to be used without control in subsequent criminal proceedings would be unjust'.[181]

12.140 An important limitation of the ALRC's recommendation was that it applied as a 'use', but not a 'derivative use', immunity. Accordingly, although the incriminating evidence itself would be inadmissible in subsequent proceedings, any evidence obtained as a result of that evidence would be admissible.[182]

12.141 Use immunities are included in a range of provisions for civil penalty proceedings—often in combination with provisions for a mandatory stay of proceedings.[183] It is unusual, however, for use immunities to be provided in the context of administrative disciplinary proceedings. One place where this has been done is disciplinary proceedings in the AFP.

12.142 Where an AFP appointee provides information, or produces a document, on the direction of a person allocated to investigate a misconduct claim:

> The information, the production of the document, record or thing, the answer to the question or the evidence obtained by doing that thing, is not admissible in evidence against the AFP appointee in any civil or criminal proceedings other than:
>
> (a) proceedings for an offence against subsection 40VH(1); or
>
> (b) proceedings in relation to termination action taken in relation to the AFP appointee; or
>
> (c) proceedings under the *Safety, Rehabilitation and Compensation Act 1988*; or
>
> (d) proceedings in tort that the AFP appointee institutes against the Commonwealth.[184]

12.143 Notably, however, the immunity only applies to information which the investigator 'expressly directed' should be produced. An AFP appointee is obliged to comply with such a direction even where it might tend to incriminate him or her, or make him or her liable to a penalty.[185] This is consistent with the common application of use immunities to mitigate the effects of a statutory abrogation of the privilege against self-incrimination and the privilege against self-exposure to penalty—for example, in the *Royal Commissions Act 1902* (Cth).[186] Use immunities have also been included in legislation that abrogates client legal privilege.[187]

---

181 Ibid, [11.75].
182 Ibid, Ch 18.
183 For example, *Fair Work Act 2009* (Cth) s 555; *Water Act 2007* (Cth) s 154; *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 183; *Broadcasting Services Act 1992* (Cth) s 205P.
184 *Australian Federal Police Act 1979* (Cth) s 40VE(4).
185 Ibid s 40VE(3).
186 *Royal Commissions Act 1902* (Cth) ss 6A, 6D. The ALRC has considered this issue in its 2009 inquiry into Royal Commissions. See also *Australian Crime Commission Act 2002* (Cth) s 30.
187 See discussion in Australian Law Reform Commission, *Privilege in Perspective: Client Legal Privilege in Federal Investigations*, ALRC 107 (2007), Ch 7.

12.144 There is some uncertainty about the application of these rights and privileges in the APS disciplinary framework.[188] A qualification to the common law right to silence applies in the employment context, through the employee's duty to comply with lawful and reasonable directions, including a direction to answer questions in disciplinary proceedings. This is generally accepted to be subject to the privileges against self-incrimination and self-exposure to penalties.[189] In the 1992 case of *Comptroller-General of Customs v Disciplinary Appeals Committee*, Gummow J, then of the Federal Court, held that the privilege against self-incrimination applied in disciplinary proceedings under the *Public Service Act 1922* (Cth).[190] The reasoning in this case appears to be reflected in the current *Public Service Act* (the successor to the 1922 Act). However, some ambiguity has arisen as a result of later decisions, which have held that the privilege against self-exposure to penalty is only applicable in judicial proceedings—which would exclude disciplinary proceedings.[191]

Submissions and consultations

12.145 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.[192]

12.146 Stakeholders expressed a range of divergent views. Some supported a requirement for a stay of administrative proceedings pending the outcome of a concurrent criminal action;[193] others, however, questioned the practicality of such an approach. In particular, concerns were raised about the delays that this could cause to the administrative process.[194] PIAC suggested that, in the alternative, consideration be given to providing for use and derivative use immunity to apply to any evidence given in such circumstances.[195]

---

188 See, eg, the comments of Flick J in *Goreng Goreng v Jennaway* (2007) 164 FCR 567, 571.

189 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor. *Police Service Board v Morris* (1985) 156 CLR 397 establishes that 'penalties' with which the privilege is concerned extend to disciplinary action in the public service.

190 *Comptroller-General of Customs v Disciplinary Appeal Committee* (1992) 35 FCR 466.

191 *Daniels Corporation International Pty Ltd v Australian Competition and Consumer Commission* (2002) 213 CLR 543, 599. See also *Rich v Australian Securities and Investments Commission* (2004) 220 CLR 129.

192 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–9.

193 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009; Australian Press Council, *Submission SR 16,* 18 February 2009.

194 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009; Australian Federal Police, *Submission SR 33,* 3 March 2009.

195 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.

12.147 The ALRC expressed the view in DP 74 that a stay of administrative proceedings would not be appropriate in relation to concurrent administrative and criminal proceedings. Instead, the ALRC proposed that the fairness of such proceedings should be enhanced by preventing evidence given by an APS employee for the purpose of administrative proceedings from being admitted in related criminal proceedings—that is, a use immunity.[196]

12.148 A number of stakeholders supported this proposal.[197] The ATO commented favourably on the potential for the proposed provision to 'ensure that employees are afforded procedural fairness in administrative proceedings, when those proceedings are running concurrently with criminal proceedings'. The Department of Defence supported the comments in DP 74 in relation to the different objects of administrative and criminal proceedings,[198] and advised that it would seek to retain 'full discretion to pursue administrative action for a breach of a secrecy provision where there is no risk of prejudicing criminal proceedings'.[199]

12.149 The ACC agreed that the proposed use immunity would help to ensure that a person who is facing disciplinary and criminal proceedings is not unfairly disadvantaged in either context. It acknowledged that public service disciplinary proceedings differ from the situation of witnesses at ACC examinations, who are required to answer all questions, including those that may be incriminatory and, by way of compensation, are entitled to a use immunity in respect of any self-incriminating evidence given. In the case of disciplinary proceedings, the employee has a choice whether to make self-incriminatory admissions. The ACC noted, however, that:

> In the absence of some form of use immunity, an employee who believes that a frank admission of the facts would best serve his or her interests in the disciplinary proceedings may be dissuaded from this course by the prospect of use of the admission in subsequent criminal proceedings.[200]

12.150 However, the ACC was concerned that a rule such as that proposed in DP 74 looked at the disciplinary process for APS employees 'solely through the prism of secrecy'. In its view, if such a rule is to be introduced, it should apply to all APS disciplinary proceedings to avoid the implication that breaches of secrecy provision merit 'special treatment' in comparison with misconduct generally. The ACC also

---

196 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 13–6.

197 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Department of Families, Housing, Community Services and Indigenous Affairs, *Submission SR 68,* 14 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

198 Department of Defence, *Submission SR 69,* 14 August 2009. See also Australian Taxation Office, *Submission SR 55,* 7 August 2009.

199 Department of Defence, *Submission SR 69,* 14 August 2009.

200 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

commented on the importance of any use immunity permitting the transfer of information to the Integrity Commissioner.[201]

12.151 Conversely, Dr Ian Turnbull did not support the proposed use immunity. He submitted that the proposal 'looks to support the privilege against self incrimination but because it also applies to other employees it simply excludes evidence from criminal trials'. Accordingly, an APS employee accused of a secrecy offence is 'in a better position' than any other accused person as regards the disclosure of Commonwealth information to prosecutors.[202]

ALRC's views

12.152 There is considerable uncertainty about how the right to silence and the privileges against self-incrimination and self-exposure to penalty apply in the context of concurrent criminal and administrative proceedings. Without further clarification, an APS employee who is subject to concurrent proceedings for breach of a secrecy provision may be dissuaded from fully participating in administrative disciplinary proceedings in order to protect his or her right to silence in the criminal context.

12.153 The ALRC has considered two options for reform in this area—a mandatory stay of administrative proceedings and a use immunity—the potential merits of which are discussed below. However, the ALRC is now of the view that the issues that are raised by concurrent disciplinary and criminal proceedings are beyond the scope of this Inquiry, and warrant consideration by the Australian Government in the context of a broader review. On this basis, the ALRC is not making a specific recommendation for reform.

Mandatory stay of proceedings

12.154 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 may stop an Australian Government agency from taking action to prevent the APS employee from making further unauthorised disclosures, which would impede the protective function of disciplinary proceedings. It may also create difficulties for the agency in successfully making out a breach of the administrative provision in the future. As has been noted in the context of concurrent criminal and legal professional disciplinary proceedings:

> The difficulty is that criminal proceedings can take years and still end inconclusively in the sense that the professionals are acquitted but concerns about their integrity or conduct *as professional*s are not resolved. In one case, the criminal trial of three lawyers accused of serious fraud did not start until almost five years after their practices had been closed down by the Law Society. Two had gained adjournments of

201 Ibid.
202 I Turnbull, *Submission SR 49,* 5 August 2009.

> their disciplinary cases, pending the outcome of the trial. They were acquitted and it was necessary to attempt to proceed with disciplinary allegations of many years' vintage.[203]

12.155 The ALRC does not consider a mandatory stay of administrative proceedings to be an appropriate safeguard for concurrent administrative and criminal proceedings for breach of a secrecy provision. It is also worthwhile to note that some concurrent criminal proceedings are expressly allowed by legislation in the context of professional disciplinary proceedings.[204]

Use immunity

12.156 The ALRC can see considerable merit in preventing certain evidence given by an APS employee in administrative proceedings for breach of a secrecy provision from being admitted in related criminal proceedings. In particular, such a reform would facilitate the full participation of an APS employee in administrative proceedings regardless of any decision to take advantage of his or her right to silence in related criminal proceedings.

12.157 It would be important to ensure that any use immunity did not unduly impinge on the conduct of related criminal proceedings. In particular, any such immunity should only apply to testimonial evidence adduced from the APS employee.[205] Arguably, much of this evidence would not currently be admissible in a criminal trial. For example, the Queensland Crime and Misconduct Commission, in its submission on proposed amendments to the use immunity in the *Independent Commission Against Corruption Act 1998* (NSW), advised that:

> at least in Queensland, most public servants are obliged to answer questions upon direction by their employer. The answers given can be used for the purposes of disciplinary proceedings. In most cases the evidence is not able to be used in criminal or civil proceedings either by statutory force or on the basis that the officer had been induced by a direction from a person in authority.[206]

12.158 The proposal in DP 74 that the *Public Service Act* should be amended to include a use immunity attracted significant stakeholder support. However, as raised by

---

203 D Middleton, 'The Legal and Regulatory Response to Solicitors Involved in Serious Fraud' (2005) 45 *British Journal of Criminology* 810, 814–815.

204 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.

205 The importance of limiting a use immunity to testimonial evidence is illustrated, eg, by the discussion in ALRC 102 about the potential for misuse of use immunities that apply to pre-existing documents in the context of disclosure orders in civil proceedings: Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005), [15.143].

206 Queensland Crime and Misconduct Commission, *Inquiry into Proposed Amendments to the Independent Commission Against Corruption Act 1988* (2009) Committee on the Independent Commission Against Corruption, <www.parliament.nsw.gov.au/icac> at 14 October 2009.

other stakeholders, any such reform raises issues outside the parameters of this Inquiry as concurrent APS disciplinary and criminal proceedings do not arise only in relation to breaches of secrecy laws.

12.159 Similar situations could arise, for example, where an APS employee is suspected of having behaved fraudulently or, as was the case in *Police Service Board v Morris*, having committed assault.[207] Concurrent disciplinary and criminal proceedings also take place in the private sector professional disciplinary context—for example, proceedings by a law society or medical board. In the ALRC's view, it is important to consider the issue of APS disciplinary proceedings for breaches of secrecy provisions in this wider context.

12.160 APS disciplinary procedures are normally conducted on a voluntary basis and in a manner that upholds the privilege against self-exposure to penalty.[208] Therefore, a broader policy question arises about whether proceedings that do not abrogate the privileges against self-incrimination and self-exposure to penalty should ever warrant the protection of a use immunity and, if so, in what circumstances. As noted above, use immunities are typically directly associated with an obligation to provide information, even where it would potentially be incriminating.

12.161 The ALRC has identified some legislation in the context of civil penalty proceedings, which provide a use immunity without also abrogating the privileges against self-incrimination and self-exposure to penalty. For example, under the *Broadcasting Services Act 1992* (Cth), the Australian Communications and Media Authority (ACMA) may apply to the Federal Court for civil penalty orders. In hearing these proceedings, the Federal Court must apply 'the rules of evidence and procedure for civil matters', which would include the privileges against self-incrimination and self-exposure to penalty.[209] The Act specifies that evidence of information given or documents produced by an individual is not admissible in criminal proceedings against the individual if:

> (a) the individual previously gave the evidence or produced the documents in proceedings for a civil penalty order against the individual for a contravention of a civil penalty provision (whether or not the order was made); and
>
> (b) the conduct alleged to constitute the offence is substantially the same as the conduct that was claimed to constitute the contravention.[210]

---

207 *Police Service Board v Morris* (1985) 156 CLR 397.

208 See P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

209 *Broadcasting Services Act 1992* (Cth) s 205K. The privileges are also retained in hearings before ACMA: see *Broadcasting Services Act 1992* (Cth) s 202(3).

210 *Broadcasting Services Act 1992* (Cth) s 205P. The immunity does not apply to a criminal proceedings in respect of the falsity of the evidence given by the individual in proceedings for the civil penalty order.

12.162 Similar frameworks apply, for example, in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth);[211] and the *Fair Work Act 2009* (Cth).[212]

12.163 As noted above, the ALRC is not recommending that a use immunity be included in the *Public Service Act* for evidence adduced in disciplinary proceedings for a suspected breach of a secrecy provision. In the ALRC's view, such a reform should be considered by the Australian Government as a component of a broader review of concurrent disciplinary and criminal proceedings, including in the professional disciplinary context.

211 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 179, 183.
212 *Fair Work Act 2009* (Cth) ss 551, 555.

13. Regulating Beyond the Australian Public Service

Contents

Introduction

13.1 In Chapter 12, 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 other statutory regimes; former employees of the Commonwealth; and individuals who are not, and have never been, in an employment relationship with the Commonwealth.

13.2 This chapter considers the administrative secrecy framework that governs Commonwealth employees engaged under a statutory regime other than the *Public Service Act*. A particular focus of recommendations is harmonising these administrative secrecy obligations with the *Public Service Act* regime.

13.3 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. The chapter makes a number of recommendations 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.

Commonwealth employees outside the APS

13.4 As discussed in detail in Chapter 12, the *Public Service Act* and related instruments establish a comprehensive administrative secrecy regime for APS employees.[1] However, many Commonwealth employees, including those who may handle some of 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);
- 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.

13.5 The disciplinary framework relevant to secrecy obligations that applies to these employees is summarised below.

Members of the ADF

13.6 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 communications with, or the giving of intelligence to, the enemy. Section 58 prohibits the unlawful disclosure of information likely to be prejudicial to the defence or security of Australia.

---

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.

13.7 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.[2]

13.8 Under the DFD Act, the manner in which a charge for breach 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 a higher order body.[3] 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.

13.9 Between 1 October 2007 and 26 August 2009, more serious service offences were tried by the Australian Military Court (AMC)—a permanent military court independent of the ADF chain of command.[4] In the case of *Lane v Morrison*, however, the High Court held that the provisions of the DFD Act that established the AMC were unconstitutional, on the basis that the AMC exercised the judicial power of the Commonwealth but did not satisfy the requirements for a federal court set out in Chapter III of the *Australian Constitution*. The Commonwealth's defence power (which had been relied on to uphold previous military justice systems) could not overcome this inconsistency.[5]

13.10 At the time of writing, the former military justice system of trials by court martial and Defence Force magistrate had been reinstated as an interim measure[6] and the Australian Government is considering options for a permanent replacement for the AMC.[7]

---

2 Parliament of Australia—Senate Foreign Affairs, Defence and Trade References Committee, *The Effectiveness of Australia's Military Justice System* (2005), [3.8].

3 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.

4 The AMC was established by the *Defence Legislation Amendment Act 2006* (Cth).

5 *Lane v Morrison* [2009] 258 ALR 404.

6 *Military Justice (Interim Measures) Act (No 1) 2009* (Cth). The *Military Justice (Interim Measures) Act (No 2) 2009* (Cth) purports to impose disciplinary sanctions on ADF members on whom the AMC imposed punishments.

7 Department of Defence, *Changes to the Military Discipline System* (2009) <www.defence.gov.au/mjs/reform.htm> at 27 October 2009.

Members of the AFP

13.11 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.[8]

13.12 The AFP Act sets out the overarching disciplinary framework for misconduct by AFP appointees. The Act provides for four categories of AFP misconduct of escalating seriousness:[9]

- Category 1: inappropriate conduct that relates to minor management or customer service matters, or reveals a need for improvement in performance;[10]
- Category 2: minor misconduct or inappropriate conduct that reveals unsatisfactory behaviour which, because of its repeated nature, warrants being treated as category 2 conduct;[11]
- Category 3: serious misconduct that raises the question whether termination action should be taken or involves a breach of the criminal law or serious neglect of duty;[12] and
- Conduct giving rise to a corruption issue.

13.13 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'.[13] 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 information', or breaching any criminal law other than one relating to Commonwealth fraud.[14]

13.14 Category 1 and 2 conduct issues are dealt with by an appointee's manager and the AFP Act sets out detailed procedural requirements for handling them.[15] These include requirements for a manager to ensure that the AFP officer and the complainant

---

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. 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.

14 Ibid.

15 *Australian Federal Police Act 1979* (Cth) pt V div 3 subdiv C.

(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.[16]

13.15 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.[17] The Commonwealth Ombudsman must also be notified of any investigation of a category 3 conduct issue.[18] 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.[19]

Employees of ASIO and ASIS

13.16 Unlike other officers of the Australian Intelligence Community (AIC),[20] employees of ASIO and ASIS are not employed under the *Public Service Act*, but rather under the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) and the *Intelligence Services Act 2001* (Cth), respectively. While ASIO and ASIS employees are subject to criminal secrecy offences,[21] no express administrative secrecy obligations or penalties are set out in their respective legislation.

13.17 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 that employment.[22] 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'.[23] ASIO has

16 Ibid s 40TJ.
17 Ibid s 40RD.
18 Ibid s 40TM(1).
19 Ibid s 40TR.
20 The AIC covers the Office of National Assessments, ASIO, ASIS, the Defence Intelligence Organisation, the Defence Signals Directorate and the Defence Imagery and Geospatial Organisation.
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).
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> at 30 November 2009. 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 the Issues Paper, *Review of Secrecy Laws* (IP 34): Australian Intelligence Community, *Submission SR 37,* 6 March 2009.

also developed a Code of Conduct to define the 'personal and professional standards' expected of ASIO officers, which includes using official information in a 'proper and reasonable manner'.[24]

13.18 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. The Director-General of ASIS is obliged, however, to consult with affected employees about these conditions.[25] 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.[26]

13.19 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.[27] 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.[28]

Employees and office holders of statutory authorities

13.20 A Commonwealth statutory authority can be defined as any public sector entity created by a specific law of the Commonwealth.[29] There are approximately 150 statutory authorities in the Commonwealth sphere, with diverse legal frameworks and governance structures.[30] In particular, there is variation in whether the authority is an agency prescribed under the *Financial Management and Accountability Act 1997* (Cth) (FMA Act)[31] or an authority subject to the *Commonwealth Authorities and Companies*

---

24 Australian Security Intelligence Organisation, *Code of Conduct* (2009) <www.asio.gov.au> at 27 October 2009.

25 *Intelligence Services Act 2001* (Cth) s 33.

26 Ibid s 355.

27 Ibid s 37.

28 Ibid s 37(3). The Director-General must also 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).

29 J Uhrig, *Review of the Corporate Governance of Statutory Authorities and Office Holders* (2003).

30 As at 1 October 2009, there were 83 agencies listed under the *Financial Management and Accountability Act 1997* (Cth) and 64 authorities under the *Commonwealth Authorities and Companies Act 1997* (Cth): Department of Finance and Deregulation, *List of Australian Government Bodies and Governance Relationships*, Financial Management Reference No 1 (2009). For a discussion of legal frameworks and governance structures, see J Uhrig, *Review of the Corporate Governance of Statutory Authorities and Office Holders* (2003).

31 Schedule 1 of the *Financial Management and Accountability Regulations 1997* (Cth) lists those bodies that are 'prescribed agencies' for the purpose of the *Financial Management and Accountability Act 1997* (Cth).

Act 1997 (Cth) (CAC Act).[32] Every Commonwealth statutory authority must operate in accordance with the governance framework set out in one of these Acts.

13.21 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.[33]

13.22 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*.[34] 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.

13.23 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 or the discretion of the authority itself (or a particular person or persons within the

---

32 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.

33 R Wettenhall, 'Exploring Types of Public Sector Organizations: Past Exercises and Current Issues' (2003) 3 *Public Organization Review* 219, 219–220.

34 The Australian Public Service Commission 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> at 23 November 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.

authority).[35] The terms and conditions of appointment of statutory office holders generally are at the discretion of the responsible minister or the Governor-General.[36]

13.24 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'.[37]

13.25 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.[38] 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.[39]

13.26 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'.[40]

---

35 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.

36 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) <www.remtribunal.gov.au> at 30 November 2009.

37 Australian Institute of Criminology, *Employee Collective Agreement 2006–2009* (2006) <www.aic.gov.au/institute/agreement/agreement.pdf> at 30 November 2009, cl 37.

38 *Australian Prudential Regulation Authority Act 1998* (Cth) s 48AC.

39 Australian Prudential Regulation Authority, *APRA Code of Conduct* (2007) <www.apra.gov.au/AboutAPRA> at 30 November 2009 under 'Standards of Conduct'.

40 Ibid.

13.27 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.[41]

13.28 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.[42] 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.[43] 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'.[44]

13.29 No equivalent obligations or penalties are set out in the FMA Act.

Ministerial staff and employees of parliamentary departments

Employees of parliamentary departments

13.30 The parliamentary departments—being the Department of the Senate, the Department of the House of Representatives and the Department of Parliamentary Services—provide information, advice and support to the Houses of Parliament, and to parliamentary committees, senators and members.

13.31 Prior to 1999, employees of the parliamentary departments were governed by the same legislation as the APS.[45] This changed with the introduction of the *Parliamentary Service Act 1999* (Cth), which established a separate framework for the employment of staff in the parliamentary departments.

---

41 Any other disciplinary actions, with the exception of formal warnings, must be approved by the relevant Executive General Manager: Ibid, 18.

42 *Commonwealth Authorities and Companies Act 1997* (Cth) s 21.

43 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.

44 *Commonwealth Authorities and Companies Act 1997* (Cth) sch 2 cl 3.

45 The governing Act was the *Public Service Act 1922* (Cth).

> 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.[46]

13.32 Under the *Parliamentary Service Act*, employees of parliamentary departments must comply with the Parliamentary Service Code of Conduct.[47] Many of the obligations imposed by this Code are equivalent to those set out in the APS Code of Conduct.[48] For example, a parliamentary departmental employee is under a duty to comply with all applicable Australian laws when acting in the course of his or her employment;[49] and to maintain 'appropriate confidentiality' about dealings that he or she has with Houses of Parliament and parliamentary committees and their members.[50]

13.33 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'.[51] A secrecy obligation is set out in cl 2.3.1 of *Parliamentary Service Determination 2003/2* (Cth), which 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.

13.34 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.[52] Procedures for determining whether an employee has breached the Code of Conduct must 'have due regard for procedural fairness' and comply with any requirements in a direction from the Parliamentary Service Commissioner.[53]

Staff of ministers and other Members of Parliament

13.35 Stakeholders in this Inquiry,[54] and other inquiries,[55] have suggested that a large number of unauthorised disclosures of official information come from ministers or ministerial advisers, for the purpose of satisfying political goals.

---

46 Explanatory Memorandum, Parliamentary Service Bill 1999 (Cth), 1.
47 *Parliamentary Service Act 1999* (Cth) s 13.
48 *Public Service Act 1999* (Cth) s 13.
49 *Parliamentary Service Act 1999* (Cth) s 13(4).
50 Ibid s 13(6).
51 Ibid s 13(13).
52 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.
53 Ibid s 15(3).
54 J Renwick, *Submission SR 02,* 11 December 2008.
55 See, eg, United Kingdom House of Commons Public Administration Select Committee, *Leaks and Whistleblowing in Whitehall*, Tenth Report of Session 2008–09 (2009), [32].

13.36 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).

13.37 In its 2003 inquiry into the framework for employment and the management of staff under the MOPS Act, 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.[56] 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.

13.38 In the specific context of ministerial staff, however, additional conduct requirements apply. The *Code of Conduct for Ministerial Staff* came into operation on 1 July 2008 and sets out the standards that ministerial staff are expected to meet in the performance of their duties.[57] 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.[58] 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 staff do not have the power to direct APS employees in their own right and that APS employees are not subject to their direction'.[59]

13.39 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'.[60]

13.40 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

---

56 Parliament of Australia—Senate Finance and Public Administration References Committee, *Staff Employed under the Members of Parliament (Staff) Act 1984* (2003), [2.13].

57 J Faulkner (Cabinet Secretary and Special Minister of State), *Code of Conduct for Ministerial Staff* (2008) <www.smos.gov.au/media/code_of_conduct.html> at 30 November 2009.

58 Ibid cll 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.

59 Ibid cl 11.

60 Ibid cl 15.

> though they may have partisan loyalties, serve the needs of their employer as a Member of Parliament.[61]

Submissions and consultations

13.41 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC expressed the view that there should be a shift in emphasis away from relying on broad criminal provisions and towards relying more heavily on administrative processes. Accordingly, the ALRC stressed the importance of having in place suitable administrative secrecy obligations, supported by just and effective procedural frameworks, for all Commonwealth employees. On this basis, the ALRC proposed that:

> 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.[62]

Framing administrative secrecy requirements

13.42 Most stakeholders that commented on this issue supported the proposal that the conduct requirement in reg 2.1 of the *Public Service Regulations* should be the standard administrative secrecy requirement applying to all Commonwealth employees.[63] The Australian Privacy Foundation agreed that the proposed approach was 'reasonable in principle', subject to its concerns with the proposed revisions to reg 2.1, discussed in Chapter 12.[64]

13.43 The Australian Crime Commission (ACC) gave in-principle support for this proposal but submitted that, in light of the sensitive nature of its information holdings, it may require more specific administrative secrecy requirements than those set out in reg 2.1.[65] The ACC also commented on its 'unusually complex employment situation', including APS employees, secondees employed under the AFP Act and other legislation, and contractors, suggesting that 'this is a clear example of the need to

---

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*, Discussion Paper 74 (2009), Proposal 14–1.

63 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

64 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

65 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

impose the same standards of conduct irrespective of the employment regime that applies to individual staff members'.[66]

13.44 Mixed staffing arrangements were also raised in an earlier submission by the Australian Securities and Investments Commission (ASIC), employees of which include both APS employees and persons employed under s 120(3) of the *Australian Securities and Investments Commission Act 2001* (Cth).[67] ASIC requires persons engaged under s 120(3) to comply with the APS Code of Conduct and other ASIC policies and procedures.[68]

Processes for investigation and enforcement

13.45 A number of stakeholders agreed that Australian Government agencies should adopt the safeguards set out in the *Public Service Act* for dealing with suspected breaches of administrative secrecy obligations, to the extent that these are consistent with the agency's functions and structure.[69] The AGD commented in its submission on IP 34 that it 'can see value' in disciplinary processes being consistent with those applicable in the APS:

> 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.[70]

13.46 However, several Australian Government agencies suggested that the proposed approach would be difficult to implement. For example, the ACC—staff of which includes APS employees, secondees, and contractors—commented that, beyond some 'core elements', in some situations 'the ideal of imposing unified processes for investigation and enforcement on a mixed workforce is unlikely to be feasible in practice'.[71] APRA noted that s 48AC of the APRA Act already sets out processes for dealing with suspected misconduct, and did not support the development of separate processes for dealing with breach of secrecy provisions.[72]

---

66 Ibid. The ACC went on to note that this complex staffing situation also demonstrates the potential difficulty of imposing unified processes for investigation and enforcement. This issue is considered below.

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

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

69 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009. See also Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009.

70 Attorney-General's Department, *Submission SR 36,* 6 March 2009. The Community and Public Sector Union 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.

71 Australian Crime Commission, *Submission SR 75,* 19 August 2009.

72 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* apply to matters other than breaches of secrecy provisions: Attorney-General's Department, *Submission SR 36,* 6 March 2009.

13.47 The Australian Privacy Foundation sought assurance that disciplinary action would be an option for 'all categories of individuals to whom the obligations applied', including ministers and ministerial staff, parliamentary staff, contractors and volunteers.[73]

ALRC's views

13.48 A key component of the ALRC's recommended regulatory framework is that—except in the most serious cases—the unauthorised disclosure of Commonwealth information should generally be dealt with through administrative processes and, where necessary, disciplinary proceedings, rather than through the criminal law. Accordingly, a sound administrative secrecy regime must be in place for all Commonwealth employees—not only APS employees.

Framing administrative secrecy requirements

13.49 The ALRC recommends that Commonwealth employees who are not employed under the *Public Service Act* should usually be subject to obligations of non-disclosure that reflect those set out in reg 2.1 of the *Public Service Regulations*, including the ALRC's recommended amendments to this regulation. This will ensure that there is 'a consistent approach across government to the protection of Commonwealth information' at the administrative level—a key objective in the Terms of Reference for this Inquiry.[74]

13.50 The ALRC notes the advice from ASIC that the staff 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. This illustrates that it will often be appropriate for equivalent administrative secrecy obligations to apply to employees inside and outside of the APS.

13.51 Moreover, the standard set out in 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 may not be applicable. 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 considers that there is no policy rationale to justify the minor differences between the wording of reg 2.1 and the administrative secrecy requirements that currently apply to employees of parliamentary departments and ministerial staff employed under the MOPS Act.

---

73 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

74 The Terms of Reference are set out at the beginning of this Report.

13.52 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 APS. 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.[75]

13.53 In the context of the ACC, the Commonwealth Ombudsman has recommended that unauthorised accessing of information should constitute 'a serious breach of ACC policy'.[76] This would reflect misconduct provisions that apply to members of the AFP. Unauthorised access, however, is not expressly covered in the APS Code of Conduct. Considering the sensitivity of much of the information held by law enforcement agencies, this may illustrate another situation where divergence from the standards set out in reg 2.1 would be warranted.

13.54 Another option to accommodate differences between the secrecy standards set out in reg 2.1 and those that are considered appropriate for particular Commonwealth employees is for an Australian Government agency to issue a direction to its staff. The role of 'lawful and reasonable directions' in administrative information-handling frameworks is considered in Chapter 14.

Processes for investigation and enforcement

13.55 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,[77] including requirements that:

- the procedure for determining whether any Australian Government employee has breached an administrative secrecy provision has 'due regard to procedural fairness';[78]

---

75 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 Neil James of the Australian Defence Association.

76 Commonwealth Ombudsman, *Australian Crime Commission: Review of the Collection, Storage and Dissemination of Information*, Report No 15 (2009), Rec 4.

77 See, eg, R Douglas and M Jones, *Administrative Law: Commentary and Materials* (3rd ed, 1999).

78 *Public Service Act 1999* (Cth) s 15(3).

- employees are given information, and a reasonable opportunity to make a statement, before a determination of breach is made;[79]

- processes for determining breaches are carried out informally and expeditiously;[80] and

- a person who determines whether an employee has breached an administrative secrecy requirement is, and appears to be, independent and unbiased.[81]

13.56 These obligations will be appropriate in the vast majority of Australian Government employment situations. In limited circumstances, however, particular features of the employing agency may warrant a different approach.

13.57 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 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.[82]

13.58 What, if any, variations are warranted should be considered by the Australian Government on an agency-by-agency basis, including any variation that may be necessary within an agency to accommodate mixed staffing arrangements such as contractors and secondees.

13.59 The ALRC's recommendation for procedural safeguards is only stated to apply to suspected breaches of secrecy provisions, in accordance with the terms of reference

---

79 *Public Service Commissioner's Directions 1999* (Cth) cl 5.2.

80 Ibid cl 5.3.

81 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.

82 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.

for this Inquiry. However, in implementing this recommendation, the Australian Government could consider applying such procedural safeguards to misconduct proceedings more broadly.

Recommendation 13–1 Australian Government agencies that employ persons other than under the *Public Service Act 1999* (Cth) should, to the extent that it is consistent with agency functions and structure:

(a) include the requirements in reg 2.1 of the *Public Service Regulations 1999* (Cth) in terms and conditions of employment; and

(b) adopt the safeguards under the *Public Service Act* for dealing with suspected breaches of reg 2.1.

Former Commonwealth employees

13.60 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 investigation into that person's conduct commenced. How, therefore, can official information held by former Commonwealth employees best be protected?

13.61 The equitable duty of confidence provides some protection for information in the hands of former employees. As discussed in Chapter 3, 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'.[83]

13.62 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.

83 *Commonwealth v Fairfax* (1980) 147 CLR 39, 52.

> 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.[84]

13.63 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.[85]

13.64 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.[86] Whether the employer 'impressed on the employee the confidentiality of the information' will also be significant.[87]

13.65 The principles set out in *Faccenda* have been followed in Australian cases such as *Wright v Gasweld Pty Ltd*[88] and *IF Asia Pacific Pty Ltd v Galbally*.[89]

13.66 An innovative legislative framework for disciplining former public servants has been introduced in the *Criminal Code and other Legislation (Misconduct, Breaches of Discipline and Public Sector Ethics) Amendment Act 2009* (Qld). Among other changes, this Act amends the *Public Service Act 2008* (Qld) to permit a chief executive to make a 'disciplinary declaration'[90] against a public servant whose employment ceases following a 'serious breach of discipline or misconduct', defined as where the

---

84 *Faccenda Chicken Ltd v Fowler* [1986] 1 All ER 617, 625.
85 Ibid, 626.
86 Ibid, 627.
87 Ibid.
88 *Wright v Gasweld Pty Ltd* [1990] NSWLR 317.
89 *IF Asia Pacific Pty Ltd v Galbally* (2003) 59 IPR 43.
90 A disciplinary declaration is a declaration of a disciplinary finding against a former public servant and the disciplinary action, including any penalty, that would have applied had the officer's employment not ended: *Criminal Code and Other Legislation (Misconduct, Breaches of Discipline and Public Sector Ethics) Amendment Act 2009* (Qld) s 20 (inserting new s 188A).

disciplinary action that would have been taken against him or her would have been termination of employment or reduction of classification level.[91]

13.67 The chief executive of a Queensland Government agency who proposes to appoint or second a person to the agency may require that person to disclose whether he or she has been subject to any 'serious disciplinary action', including a disciplinary declaration.[92] A chief executive can also ask the chief executive of another Queensland Government agency for information about any disciplinary declaration that has been issued against a former employee of that agency, where it is reasonably necessary for making an employment decision or a disciplinary finding.[93]

Submissions and consultations

13.68 In DP 74, the ALRC expressed the preliminary view that it would not be feasible to impose ongoing administrative secrecy obligations on former Commonwealth employees, because of the lack of a continuing statutory relationship to support the imposition of disciplinary penalties. Instead, the ALRC proposed that criminal secrecy offences and the equitable duty of confidence should be relied on in this context. In order to promote the deterrent effect of these laws, the ALRC proposed that Australian Government agencies should remind employees, on termination, of their continuing legal responsibilities.[94]

13.69 Those stakeholders that made submissions on this proposal expressed unanimous support.[95] For example, the Australian Taxation Office (ATO) commented on the importance of former officers being aware that taxpayer information to which they had access while employed with, or contracted by, the ATO, remains protected by the operation of tax law secrecy provisions.[96]

13.70 In its submission in response to IP 34, 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'.[97]

---

91 Ibid s 20. The same substantive system has also been established under the *Police Service Administration Act 1990* (Qld).

92 Ibid s 12 (inserting new s 179A).

93 Ibid s 20 (inserting new s 188B).

94 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 14–2.

95 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

96 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

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

ALRC's views

13.71 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, which, in the case of former employees, no longer exists. Further, the penalties that may be imposed under administrative disciplinary regimes have little, if any, practical application where there is no ongoing employment relationship with the Commonwealth.[98] The ALRC has focused, therefore, on ensuring that employees are aware, at the time that employment is terminated, of their continuing secrecy obligations under other laws, including the equitable duty of confidence, the recommended general secrecy offence and any specific secrecy offences.

13.72 In the ALRC's view, reinforcing the potentially serious consequences of any unauthorised disclosures of Commonwealth information at the time of separation—for example, during an employee's exit interview—can play a valuable role in deterring former Commonwealth employees from engaging in such conduct. It also provides an opportunity for Australian Government agencies to reinforce the personal nature of non-disclosure obligations.

13.73 The ALRC can see merit in the 'disciplinary declaration' scheme introduced in Queensland through the *Criminal Code and Other Legislation (Misconduct, Breaches of Discipline and Public Sector Ethics) Amendment Act*. The ALRC has not had the opportunity to consult on the scheme and, on this basis, is not recommending that an equivalent be introduced at the Commonwealth level. However, the Australian Government may wish to give further consideration to adopting aspects of this scheme in relation to breaches of secrecy provisions, or misconduct more generally, by former Commonwealth employees.

Recommendation 13–2 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

13.74 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:

98 Penalties for breach of the APS Code of Conduct are discussed in Ch 12.

- 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 statutory or contractual relationship to the Commonwealth.

Contracted service providers

Background

13.75 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.[99] Many of these contracts are with private sector service providers.[100]

13.76 Depending on the services being rendered, a contracted service provider could be given access to extensive and/or highly sensitive Commonwealth information. 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 Australian Government 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.

13.77 In other situations, the information warranting protection may be generated by the contracted service provider itself, for example, where contractors are responsible for providing immigration detention services, and subcontractors are responsible for providing health services to detainees of the (now closed) Baxter Detention Centre.[101]

13.78 In such circumstances, the principal mechanism of controlling the flow of Commonwealth information is contractual.

13.79 At a practical level, the ALRC has heard that information sharing between Australian Government agencies and contracted service providers generally works

---

99 Department of Finance and Deregulation, *Statistics on Australian Government Procurement Contracts* (2009) <www.finance.gov.au/publications/statistics-on-commonwealth-purchasing-contracts/index.html> at 30 November 2009.

100 Other than the private sector, the Australian Government may also enter into contracts with Commonwealth statutory entities and state and territory departments and entities.

101 A description of the contractual 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.

well, with one of the major providers advising that it has not encountered any situations where agencies have been unwilling to share confidential information that was necessary for it to adequately perform its services.[102]

Guidance on Confidentiality in Procurement (FMG 3)

13.80 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 agency contracts.

Confidential information

13.81 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.[103]

13.82 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 confidentiality requirement, an Australian Government agency may determine information under a contract that should be kept confidential. However, an agency does not have unlimited discretion in making such a determination:

> 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 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.[104]

13.83 The FMG 3 suggests that one situation where it may be appropriate for an Australian Government agency to determine that information should be treated as confidential under a contract is where disclosure would be contrary to the public

---

102 PricewaterhouseCoopers, *Submission SR 53,* 7 August 2009.

103 Australian Government Department of Finance and Administration, *Financial Management Guidance No 3: Guidance on Confidentiality in Procurement*, 1 July 2007, [3.1].

104 Australian Government Solicitor, *Legal Briefing No 64: Identifying and Protecting Confidential Information* (2002). This also considers the circumstances in which an equitable obligation to protect information arises in the absence of a contract. 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).

interest—for example, because it could compromise national security or defence or disclose Cabinet deliberations.[105]

Confidential Commonwealth information

13.84 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. What may be less clear, however, is the status of information prepared by a contracted service provider for the purposes of the contract, the use and disclosure of which an Australian Government agency may seek to control. The question, therefore, is when will 'confidential information' also be 'confidential Commonwealth information'?

13.85 The model confidentiality clause for contracts 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'.[106] The FMG 3 does not specify what information will be 'of the other Party'.

Exceptions to the obligation of confidentiality

13.86 The model confidentiality clause in the 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;
- disclosed as authorised or required by law; or
- otherwise in the public domain.[107]

---

105 Other situations include, eg, where the Australian Government will hold intellectual property rights over the information; or the contracted service provider demonstrates that the commercial sensitivity of the information warrants confidentiality: Australian Government Department of Finance and Administration, *Financial Management Guidance No 3: Guidance on Confidentiality in Procurement*, 1 July 2007, [3.9]–[3.14].

106 Ibid, Appendix B, cl B3(1.1.1) (emphasis added).

107 Ibid, Appendix B, cl B3(1.3.1). Exceptions also apply to permit the Commonwealth to disclose information to the responsible minister, or a House or Committee of Parliament or to share information within the Commonwealth to serve legitimate interests.

Binding individual employees

13.87 As noted by the Australian Government Solicitor (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.[108]

13.88 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.[109]

13.89 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 are trained in how to use the information in compliance with the agreement.[110]

13.90 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. The FMG 3 suggests that an undertaking is likely to be relevant:

---

108 A Snooks, *Commercial Notes No. 25: Protecting Commonwealth Information* (2008).

109 Ibid.

110 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.

> 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.[111]

13.91 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 3, equity may provide a remedy for the unauthorised use of confidential information 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.

13.92 Finally, in some circumstances, the recommended general secrecy offence will apply to a person who discloses Commonwealth information that he or she obtained under a contract for services.[112] Specific secrecy offences may also be relevant.[113] The ALRC is also recommending that subsequent disclosure offences should apply in certain circumstances.[114]

Applying the APS Code of Conduct

13.93 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 confidential Commonwealth 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.[115]

---

111 Australian Government Department of Finance and Administration, *Financial Management Guidance No 3: Guidance on Confidentiality in Procurement*, 1 July 2007, 39.

112 The elements of the general secrecy offence are discussed in Ch 6.

113 Specific secrecy offences are discussed in Chs 8–11.

114 Recommendations 6–6, 6–7.

115 Victorian Government State Services Authority, *Code of Conduct for Victorian Public Sector Employees* (2007) <www.ssa.vic.gov.au/> at 4 December 2009, [1.4].

Approach in DP 74

13.94 In DP 74, the ALRC acknowledged the importance of protecting Commonwealth information that is disclosed to, or generated by, private sector contracted service providers and subcontractors through clearly drafted confidentiality clauses. The ALRC also noted, however, that contractual requirements only apply to the contracting organisation itself, not to employees who deal with the information. To ensure that Commonwealth information in the hands of contracted service providers received robust protection, the ALRC proposed that Commonwealth contracts should include confidentiality clauses that:

- clearly set out the categories of information that are confidential Commonwealth information; and

- require persons (other than Commonwealth employees) who have access to the information because of the contract to agree to comply with contractual confidentiality obligations.[116]

13.95 The ALRC further proposed that contracts should expressly permit the disclosure of confidential Commonwealth information where this would amount to a public interest disclosure under the proposed Commonwealth public interest disclosure legislation.[117]

13.96 Beyond any obligations set out in the contract, the ALRC sought to ensure that employees of contracted service providers who have access to Commonwealth information are aware of the circumstances in which liability could result. In particular, the ALRC proposed that private sector providers should take steps to make their staff aware of their obligations of secrecy—and, in particular, any relevant criminal offences.[118] This proposal aimed to promote the deterrent effect of secrecy offences, as well as recognising the undesirability of imposing criminal sanctions on a person who was unaware of his or her potential liability.

Submissions and consultations

13.97 A number of stakeholders supported the ALRC's proposed approach to contracted service providers and their personnel.[119] The ACC, for example, suggested

---

116 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 14–3.

117 Ibid.

118 Ibid, Proposal 15–7.

119 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Australian Crime Commission, *Submission SR 75,* 19 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

that the proposed contractual provisions would have the benefit of allowing contractors to be given a 'fully effective briefing' about relevant ACC information.[120]

13.98 The ATO generally supported the proposal for contractual confidentiality provisions; however, it submitted that clearly setting out categories of information that are confidential may raise practical difficulties in some situations. The ATO also advised that an explanation of the role and operation of tax law secrecy provisions constitutes a standard clause in contracts with external service providers. Therefore, as a matter of practice it ensures that service providers are aware that taxpayer information is subject to ongoing protection under tax law secrecy provisions and that breach of these provisions could result in criminal prosecution.[121]

13.99 Several submissions also commented on the relationship between contractual confidentiality provisions and the ALRC's broader regulatory framework. For example, the Australian Privacy Foundation noted that mechanisms such as contractual provisions and confidentiality agreements were important compensation for the repeal of secrecy provisions in some individual laws.[122] In its submission in response to IP 34, the DHS noted the importance of contracted service providers and subcontractors appreciating the personal nature of their secrecy obligations.[123]

13.100 The Australia's Right to Know coalition was concerned about the potential for confidentiality provisions in Commonwealth contracts to be cast too broadly:

> 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.
>
> 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.[124]

ALRC's views

13.101 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. Contracted service providers may be sued for breach of contract for inappropriate disclosures, or remedies in an action for

---

120 Australian Crime Commission, *Submission SR 75,* 19 August 2009.
121 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
122 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.
123 Department of Human Services, *Submission SR 26,* 20 February 2009.
124 Australia's Right to Know, *Submission SR 72,* 17 August 2009; Australia's Right to Know, *Submission SR 35,* 6 March 2009.

breach of confidence. As stakeholders noted, this may be particularly important in the context of the ALRC's recommendations for narrowing the scope of the general secrecy offence, and narrowing the scope of and repealing many specific secrecy offences.[125]

13.102 There was broad stakeholder support for including in contracts the categories of information that are 'confidential Commonwealth information'. This could include, for example, personal taxation information or security classified information. However, the ALRC agrees with the ATO that sometimes it will be preferable to identify confidential information in some other way than categories of information. For example, where a contracted service provider is only being provided with one Commonwealth dataset, then the contract could specifically identify this dataset as confidential rather than attempting to delineate a more general category. Accordingly, the ALRC recommends that Commonwealth contracts should set out the 'information or categories of information' that are confidential Commonwealth information.

13.103 One limitation of contractual requirements is that they only apply to the contracting organisation itself—no obligations are directly imposed on employees who deal with the information. The ALRC is making two recommendations to impress upon employees and others their personal responsibilities for protecting information received under a contract with the Australian Government. First, 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 contractual confidentiality requirements. Secondly, contracted service providers 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 or civil liability could result.

13.104 The ALRC is not recommending that contracts for services should include, as a matter of course, a requirement for personnel to comply with the APS Code of Conduct. It will often be unreasonable to expect contracting personnel to ascertain the circumstances when disclosure of information is likely to be prejudicial to 'the effective working of government'.[126] Further, where a contract involves access only to limited Commonwealth information, it will usually be clearer to identify the precise information that is the subject of protection.

13.105 Nor is the ALRC specifying the way in which the agreement of personnel should be sought. Normally it will 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

125 The general secrecy offence is discussed in Chs 5–7. Specific secrecy offences are discussed in Chs 8–11.
126 The duty of non-disclosure in the APS Code of Conduct is discussed in detail in Ch 12.

signed deed of confidentiality. The option to require such a deed is already made clear in the FMG 3 and, therefore, is not the subject of an ALRC recommendation.

13.106 Finally, in the ALRC's view, contracted service providers and subcontractors should be shielded from civil or criminal liability for the disclosure of Commonwealth information where this is in accordance with 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 contractors and consultants engaged by the public sector and their employees should be entitled to make a protected disclosure.[127] Flowing on from this immunity, contractual confidentiality clauses should include an exception for conduct that amounts to a public interest disclosure under public interest disclosure legislation.

Recommendation 13–3 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 information or 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 is protected under Commonwealth public interest disclosure legislation.

Recommendation 13–4 Private sector organisations that perform services for or on behalf of the Australian Government under contract should ensure that all employees who have access to Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal and civil liability could result.

127 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.

Members of boards and committees

13.107 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.[128]

13.108 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. 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, including comparisons between the clinical benefits of the product and other similar pharmaceuticals and an evaluation of the economic implications of listing the product on the PBS.[129]

13.109 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 the responsible minister. The establishing legislation, however, often provides for the prospect of termination of membership in the event of 'misbehaviour'.[130]

13.110 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.

---

128 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.

129 Department of Health and Ageing, *Guidelines for preparing submissions to the Pharmaceutical Benefits Advisory Committee (Version 4.3)* (2004) <www.health.gov.au/internet/main/publishing.nsf/content/pbacguidelines-index> at 30 November 2009.

130 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).

13.111 Some members of boards and committees serve in an ex officio capacity—automatically appointed by reason of their office. For example, s 7B of the *Australian Crime Commission Act 2002* (Cth) establishes the membership of the board of the ACC as being:

> (a) the Commissioner of the Australian Federal Police;
>
> (b) the Secretary of the Department;
>
> (c) the Chief Executive Officer of Customs;
>
> (d) the Chairperson of the Australian Securities and Investments Commission;
>
> (e) the Director-General of Security holding office under the Australian Security Intelligence Organisation Act 1979;
>
> (f) the Commissioner or head (however described) of the police force of each State and of the Northern Territory;
>
> (g) the Chief Police Officer of the Australian Capital Territory;
>
> (h) the CEO.

13.112 Certain disclosures of Commonwealth information by members of boards and committees will be restrained by the equitable duty of confidence. In some circumstances, the recommended general secrecy offence, subsequent disclosure offences and specific secrecy offences may also be relevant.[131]

Submissions and consultations

13.113 In DP 74, the ALRC proposed that the Australian Government should include secrecy requirements in the terms and conditions of appointment for members of boards and committees. The ALRC expressed the preliminary view that these should be equivalent to the secrecy requirements that would apply to Commonwealth employees in a related employment context—which would usually mean reg 2.1 of the *Public Service Regulations*—to the extent that this would be consistent with the board's or committee's functions and structure.

13.114 A number of stakeholders supported this proposal.[132] The ATO agreed that if a member of a board or committee was successfully prosecuted for breach of a tax law secrecy provision then it would support that member's tenure being terminated.[133]

ALRC's views

13.115 Members of Commonwealth boards and committees will often have access to sensitive information. It is important, therefore, to make sure that these members are

---

131 The general secrecy offence and subsequent disclosure offences are discussed in Chs 5–7. Specific secrecy offences are discussed in Chs 8–11.

132 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

133 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

subject to sufficient requirements of confidentiality. A logical location for these is in the terms and conditions of appointment.

13.116 In the ALRC's view, equivalent secrecy requirements should be imposed 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 secrecy obligations equivalent to those that apply to employees of the Therapeutic Goods Administration, which provides the secretariat for PBAC.

13.117 Often this will mean that members of boards and committees will be subject to a duty of non-disclosure analogous to that set out in reg 2.1 of the *Public Service Regulations*—that is, where the disclosure is reasonably likely to be prejudicial to the effective working of government and does not fall within any of the relevant exceptions. Where the most closely related Commonwealth employment situation for a board or committee involves different non-disclosure requirements from those set out in reg 2.1, those different obligations are also likely to be appropriate for the board or committee.[134]

13.118 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.

13.119 In order to ensure that there is a mechanism to enforce the obligation of secrecy, the terms and conditions of appointment of members of Commonwealth boards and committees should specify the right to terminate the member for breach. The termination provision serves a protective function analogous to disciplinary proceedings for Commonwealth employees and, accordingly, should be accompanied by timely and effective processes for making determinations of breach.

13.120 Where a board or committee member discloses Commonwealth information and that disclosure caused, or was reasonably likely, or intended to cause, harm to an essential public interest, he or she may also be subject to criminal proceedings for breach of the recommended general secrecy offence,[135] the subsequent disclosure offences,[136] and/or specific secrecy offences.[137] At the time of appointment, the Australian Government should make members aware of their potential liability in this

---

134 Situations in which the obligation of non-disclosure that applies to a Commonwealth employee may differ from reg 2.1 are discussed above.

135 Recommendation 6–1. Members of Commonwealth boards and committees may fall within 'individuals who exercise powers, or perform functions, conferred on them by or under a law of the Commonwealth'.

136 Recommendations 6–6, 6–7.

137 Specific secrecy offences are discussed in Chs 8–11.

regard. This is important to promote the deterrent function of the criminal law. It also recognises the undesirability of imposing criminal sanctions on a person who was unaware of his or her potential liability. Members of boards and committees should also be advised of their obligations under the equitable duty of confidence.

13.121 As noted by the ACC, ex officio members are largely unaffected by the ALRC's recommended framework for boards and committees. The responsible minister or agency has no discretion as regards the appointment of the office-holder to the board or committee and, consequently, is not empowered to terminate his or her membership. This may be especially troubling where the position held by an ex officio member is outside the Australian Government altogether—for example, a state or territory public servant—and, on this basis, is not covered by other disciplinary avenues in the Australian Government.[138] The ALRC's recommendation that the Australian Government should raise awareness of board and committee members' obligations of secrecy under the equitable duty of confidence and general and specific secrecy offences will be especially important in the case of ex officio members.

Recommendation 13–5 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) a right to terminate the appointment of a member in the event of a breach of the secrecy obligation.

Recommendation 13–6 The Australian Government should ensure that members of boards and committees who have access to Commonwealth information are aware of their obligations of secrecy, including the circumstances in which criminal and civil liability could result.

State and territory public sector employees

13.122 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 New South Wales (NSW), for example, the *Model Code of Conduct for NSW Public Agencies*, issued by the Department of Premier and Cabinet, requires

138 However, where the office-holder is a state or territory public servant, the disclosure may constitute a breach of secrecy obligations that apply to his or her substantive position, and result in disciplinary proceedings by the state or territory government. Secrecy obligations in state and territory public sectors are discussed below.

NSW Government agencies to have in place 'clearly documented procedures regarding the storage, disclosure and distribution of confidential or sensitive personal, commercial or political information'.[139] 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'.[140]

13.123 The Victorian public sector is governed by the *Code of Conduct for Victorian Public Sector Employees*.[141] 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.[142]

13.124 South Australia has in place the most detailed codification of the circumstances in which 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

---

139 New South Wales Premier's Department, *Model Code of Conduct for NSW Public Agencies* (1997), 6.

140 Ibid.

141 Victorian Government State Services Authority, *Code of Conduct for Victorian Public Sector Employees* (2007) <www.ssa.vic.gov.au/> at 4 December 2009.

142 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.[143]

13.125 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'.[144] The *State Service Act 2000* (Tas) requires Tasmanian public servants to maintain 'appropriate confidentiality' about information that they acquire in the course of employment.[145] Public sector obligations under 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'.[146]

13.126 The Queensland regime focuses on the procedure for developing public sector codes of conduct, as opposed to the substantive content of agency codes.[147] 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.[148]

13.127 All Australian governments have agreed through a memorandum of understanding to comply with the minimum protective security standards contained in the *Australian Government Protective Security Manual* (PSM) for handling national security information.[149]

ALRC's views

13.128 In DP 74, the ALRC expressed the preliminary view that there was no need to reform the administrative framework for state and territory public sector employees who access Commonwealth information. These persons are subject to state and

---

143 *Public Sector Management Regulations 1995* (SA) reg 15.

144 *Public Sector Management Act 1994* (ACT) s 9.

145 *State Service Act 2000* (Tas) s 9.

146 *Public Service Regulations 1988* (WA) reg 8.

147 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.

148 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.

149 See New South Wales Department of Premier and Cabinet, *NSW Policy and Guidelines for Protecting National Security Information*, M2008–17 (2008).

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. The submissions on DP 74 did not raise any further concerns in this regard.

13.129 Accordingly, the ALRC is not making any recommendations for reform to the administrative framework for state and territory public sector employees who access Commonwealth information.

No statutory or contractual relationship with the Commonwealth

13.130 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 unauthorised disclosure of certain information by Ms Tjanara Goreng Goreng to her daughter and to a member of the administration of an Indigenous community.[150] Although both criminal and administrative disciplinary penalties were applicable 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.

13.131 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 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.[151]

13.132 In DP 74, the ALRC asked 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.[152] Only one

150 *R v Goreng Goreng* [2008] ACTSC 74.
151 Australian Press Council, *Submission SR 16,* 18 February 2009.
152 Australian Law Reform Commission, Review *of Secrecy Laws*, Discussion Paper 74 (2009), Question 14–1.

stakeholder addressed this question, advising that it did not see a need for civil penalties in this area.[153]

13.133 The limited response from stakeholders on this question seems to indicate that there are not significant problems in this area. Accordingly, the ALRC is not making a recommendation for reform in this regard. The subsequent disclosure offences recommended by the ALRC in Chapter 6 would apply to the subsequent unauthorised disclosure of Commonwealth information by non-Commonwealth officers where the information has been supplied in confidence or in breach of the general secrecy offence.[154]

153 Australian Crime Commission, *Submission SR 75,* 19 August 2009.
154 Recommendations 6–6, 6–7.

14. Frameworks for Effective Information Handling

Contents

Introduction

14.1 Previous chapters of this Report have focused on the legal obligations of non-disclosure that should apply 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 agencies and organisations.

14.2 Australian Government agencies employ a range of strategies to guide the release of Commonwealth information by individual officers, including developing and

implementing written manuals, policies 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) and agency policies on information handling. In some situations, Australian Government agencies may issue directions to employees, which impose new and different legal obligations from those set out in secrecy and other information-handling laws. Information-sharing practices may be formalised through memorandums of understanding (MOUs) and information and communication technology (ICT) systems.

14.3 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 improvements.

14.4 Chapter 15 considers issues relating to the information-handling culture of an Australian Government agency—including, for example, the training and education of employees and avenues for employees to raise queries and concerns. The chapter also discusses the role of integrity agencies in overseeing the manner in which agencies discharge their information-handling responsibilities.

14.5 The relationship between secrecy laws and other laws relevant to information handling is discussed in Chapter 16.

Commonwealth information-handling manuals

14.6 Several policies that operate across the Australian Government apply to information handling. Of particular relevance are the PSM and the *Australian Government Information and Communications Technology Security Manual* (ACSI 33).

Australian Government Protective Security Manual

14.7 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.[1] 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.

14.8 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:

---

1 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual (PSM) [Summary]* (2006) <www.ag.gov.au> at 30 November 2009.

- 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;

- once information has been identified as requiring security classification, a protective marking must be assigned to the information; and

- once information has been security classified, agencies must observe the minimum procedural requirements for its use, storage, transmission and disposal.[2]

14.9 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.[3]

14.10 '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;

---

2 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.

3 Ibid, [2.9].

- **Highly Protected**—if compromise of it could cause 'serious damage' to the Commonwealth, the Government, commercial entities or members of the public.[4]

14.11 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 that he or she would be a security risk.[5]

14.12 The Australian Government's stated policy is to keep security classified information to the necessary minimum.[6] However, in a 1999 report on the operation of the classification system for protecting sensitive information, the Australian National Audit Office (ANAO) noted that all audited agencies incorrectly classified files, with over-classification being the most common occurrence.[7]

14.13 Ongoing concerns about the classification system were also raised in a number of submissions to this Inquiry.[8] Civil Liberties Australia (CLA) suggested that, in classifying information, the default position should be 'totally free access':

> CLA advocates a system of levels of classification related to purpose (as outlined above), and not to pejorative words such a 'Secret' and 'Top Secret'. These are myth-based categories stemming from world wars in the past century, or even earlier. The entire notion of information has changed since then, as has the speed of delivery, the power of search, the contraction of the tyranny of distance and the explosion of education and general knowledge.[9]

14.14 The Australian Press Council submitted that there should be rules that strictly define the parameters of what should be kept secret to stop the over-classification of material. These should include a provision making it an offence to withhold information from the public for an improper purpose.[10]

14.15 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;[11]

---

4 Ibid, [2.12].
5 Ibid.
6 Ibid, [2.10].
7 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Audit Report 7 (1999), [2.84].
8 See, eg, 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.
9 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
10 Australian Press Council, *Submission SR 62,* 12 August 2009.
11 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;[12] 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.[13]

14.16 The ALRC further recommended that the PSM (with any sensitive protective security information removed) should be placed in the public domain[14]—as is the case in most comparable jurisdictions, such as the United States, Canada and New Zealand.[15]

14.17 The PSM has been revised since the publication of ALRC 98 and, contrary to the ALRC's recommendation, the entire document was given a security classification. In a submission to this Inquiry, Liberty Victoria commented that the 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'.[16]

14.18 Questions have been raised about the potential for PSM requirements to inhibit effective information sharing. For example, in its audit of the 2008–09 financial statements of Australian Government agencies, the ANAO observed instances where the Australian Taxation Office (ATO) was not complying with requirements of the PSM with respect to the classification, storage and distribution of protected information.[17] In an article in the *Australian Financial Review*, the ATO defended its practices on the basis that the residual risk 'represents the best possible trade-off between the community benefits, costs and risks of any alternative approach', for example, by allowing the ATO to communicate with taxpayers through unencrypted emails where there was no other alternative.[18]

ALRC's views

14.19 Shortcomings in the drafting or application of the PSM have the potential to detract from many of the recommendations for reform set out in this Report. For example, the over-classification of information, or a failure to declassify information,

---

12 Ibid, Rec 4–4.
13 Ibid, Rec 4–5.
14 Ibid, Rec 4–1. At the time of ALRC 98, the PSM did not have a security classification but was not publicly available.
15 Ibid, [4.17].
16 Liberty Victoria, *Submission SR 19,* 18 February 2009. See also Australian Press Council, *Submission SR 16,* 18 February 2009, which also called for the PSM to be declassified and made publicly available.
17 Australian National Audit Office, *Interim Phase of the Audit of Financial* (2009), [4.428].
18 F Anderson, 'Taxpayer Data at Risk: Audit', *Australian Financial Review*, 15 July 2009, 3.

could prevent information sharing for the purpose of whole of government initiatives.[19] Unwarranted security classifications may also mean that information is not made publicly available where this could appropriately be done, thereby detracting from the principle of open government.

14.20 The ALRC affirms its support for the recommendations in ALRC 98 in relation to the PSM.[20] In particular, the ALRC remains of the view that the PSM (with any sensitive protective security information removed) should be made publicly available.[21]

Australian Government Information Security Manual

14.21 ACSI 33, issued by the Defence Signals Directorate, complements the PSM by assisting Australian Government agencies to achieve sound information and communications technology (ICT) security.[22] ACSI 33 sets out baseline requirements for ICT security, along with a framework for governance of ICT security within Australian Government agencies. In meeting these standards, agencies are directed to the principles for information security established by the Organisation for Economic Co-operation and Development including, for example, that:

- participants should be aware of the need for security of information systems and networks and what they can do to enhance security;
- participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents;
- the security of information systems and networks should be compatible with essential values of a democratic society;
- participants should incorporate security as an essential element of information systems and networks; and
- participants should adopt a comprehensive approach to security management.[23]

14.22 These standards and principles will operate alongside specific information-handling policies adopted in particular Australian Government agencies, considered below.

---

19 Whole of government is discussed in Ch 2.

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

21 Ibid, Rec 4–1.

22 Australian Government Defence Signals Directorate, *Australian Government Information Security Manual (ACSI 33)* (2009).

23 Ibid.

Agency-specific policies and guidelines

14.23 Agency policies and guidelines will typically be the first point of call for Commonwealth employees seeking to understand their information-handling obligations.

14.24 The guide issued for Australian Public Service (APS) employees by the Australian Public Service Commission, *APS Values and Code of Conduct in Practice*, advises that:

> 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.[24]

14.25 The potential for agency policies or guidelines to operate as a 'lawful and reasonable direction' to an employee and thereby impose new legal obligations on employees is discussed in the following section of this chapter.

Role of agency policies and guidelines

Clarifying the application of relevant secrecy laws

14.26 A key role of agency policies and guidelines is to clarify the application of relevant secrecy laws to the information holdings of an Australian Government agency. This may promote effective information handling by Commonwealth employees, informing and instilling confidence in agency employees and others about the types of information that can be disclosed and the processes for disclosure.

14.27 For example, agency policies and guidelines can clarify the disclosures that may be reasonably likely to prejudice the 'effective working of government', and, accordingly, be in breach of reg 2.1 of the *Public Service Regulations 1999* (Cth).[25] Some guidance in this regard is available in *APS Values and Code of Conduct in Practice*:

> Depending on the circumstances, this restriction could cover information, such as opinions, consultation, negotiations (including about the management of a contract),

---

24 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009, Ch 3.

25 In Ch 12, the ALRC makes a number of recommendations for reform of reg 2.1.

> incomplete research, or advice or recommendations to the Government, leading or related to, the development or implementation of the Government's policies or programmes. …
>
> The exemptions set out in the [*Freedom of Information Act 1982* (Cth)] are a useful starting point in determining which categories of information may potentially fall within the scope of regulation 2.1.[26]

14.28 Agency policies and guidelines may also clarify the scope of exceptions to secrecy laws for disclosures made 'in the course of an officer's duties'—as found, for example, in reg 2.1 of the *Public Service Regulations* in addition to many criminal secrecy offences. The ALRC recommends a continuing role for such an exception in the context of the general secrecy offence and specific secrecy offences.[27]

14.29 In other situations, an Australian Government agency may issue a policy to deal with a specific contentious or problematic issue. This is illustrated, for example, by the 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.[28]

14.30 The importance of having in place overarching information-handling policies was stressed in the 2009 report by the Commonwealth Ombudsman on the collection, storage and dissemination of information by the Australian Crime Commission (ACC), which followed a leak to the media of information that the ACC held about a minister. The Ombudsman criticised the disjointed and inconsistent nature of ACC information governance policies and recommended that:

> The ACC should make the development of an overarching information governance policy a high priority. The policy needs to be coherent, take account of existing effective operational practices, be appropriately clear and concrete, balance the benefits of information sharing with the need-to-know principle, provide advice regarding access controls, outline audit functions and provide appropriate definitions and clear advice on sanctions.[29]

14.31 Because policies and guidelines reflect a broad set of information-handling laws and objectives, their requirements may appear inconsistent with those set out in related secrecy laws. In particular, tensions can arise 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 Committee heard evidence about the Department of Defence's

---

26 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009.

27 Recommendations 7–1, 10–2.

28 Australian Taxation Office, *ATO Practice Statement Law Administration: Disclosure to Ministers about the Affairs of Taxpayers*, PS LA 2004/9 (2004).

29 Commonwealth Ombudsman, *Australian Crime Commission: Review of the Collection, Storage and Dissemination of Information*, Report No 15 (2009), Rec 1.

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.[30]

14.32 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 1976* (Cth) 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 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.[31]

14.33 In comparison, an agency may seek to lessen legislative standards of secrecy by seeking to expand, through policy documents, an exception to secrecy laws for conduct in the course of an officer's duties. This issue was considered by the Australian Government Solicitor (AGS) in its advice to the ATO on the secrecy provision in s 16 of the *Income Tax Assessment Act 1936* (Cth), which includes an exception for conduct in 'the performance of the person's duties as an officer':

> On an ordinary interpretation of the phrase 'duties', one might come to the conclusion that it includes all functions a person undertakes consistently with direction from their superiors. The caselaw considering this phrase has interpreted it broadly. However, there are limitations to the duties that are contemplated by s 16. …
>
> In our view, a person's duties under s 16(2A) cannot include policy obligations imposed by a Minister by way of a policy document such as the Fraud Control Guidelines or the Commonwealth Prosecutions Policy. If an officer's duties could extend so far, nothing would prevent the Executive from circumventing a restriction set down by Parliament (the secrecy provisions) simply by making a policy permitting disclosure in the desired circumstances. Parliament, in enacting s 16, could not have intended that future governments would be able to widen the circumstances in which information could be disclosed simply by issuing a policy document.[32]

Transparency

14.34 Some stakeholders in submissions in response to the Issues Paper, *Review of Secrecy Laws* (IP 34),[33] remarked on the potential role of agency policies and guidelines in assisting members of the public to understand the standard of openness

---

30 Parliament of Australia—Senate Select Committee on a Certain Maritime Incident, *Majority Report* (2002), [2.53].

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

32 D Boucher, *Report of a Review of Information Handling Practices in the Serious Non Compliance Business Line of the Australian Taxation Office* (2008), Attachment 9, 22.

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

that they should expect from government.[34] The Australian Press Council noted, for example, that this would facilitate actions for judicial review and 'enable citizens to develop an understanding of the extent and character of secrecy processes'.[35] 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.[36]

Approach in Discussion Paper

14.35 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC proposed that Australian Government agencies should develop and implement policies clarifying the application of relevant secrecy laws and other information-handling obligations to their information holdings, including, at a minimum, information about:

- the types of information that an employee can lawfully disclose in the performance of his or her duties;
- the types of information for which an employee must obtain authority for disclosure;
- the circumstances in which the unauthorised handling of information could result in disciplinary action;
- the circumstances in which the unauthorised handling of information could lead to criminal proceedings; and
- avenues for an employee to raise queries or concerns, including the process by which he or she can make a public interest disclosure.[37]

14.36 In formulating this proposal, the ALRC distinguished the role of policies and guidelines in clarifying the application of secrecy laws and other information-handling obligations from that of imposing new and different legal requirements. The ALRC expressed the view that if agency information-handling policies are drafted correctly, they will normally set out a level of secrecy equivalent to that set out in related Commonwealth secrecy laws. In certain circumstances, however, other legal requirements—for example, a requirement for information to be accurate—may justify an agency imposing a different level of secrecy. To be characterised as clarification, these discrepancies must be justified on the basis of other legal requirements.

---

34 Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009; Australian Press Council, *Submission SR 16,* 18 February 2009.

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

36 Ibid.

37 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 15–1.

14.37 The ALRC also noted the public information role of agency policies and guidelines and, to this end, proposed that—save in certain exceptional cases where it would be unreasonable or impractical—Australian Government agencies should make their information-handling policies publicly available.[38]

Submissions and consultations

Clarifying the application of relevant secrecy laws

14.38 A number of stakeholders supported the ALRC's proposal that Australian Government agencies should develop policies that clarify the application of relevant secrecy laws to their information holdings, including baseline requirements for information that must be included in these policies.[39]

14.39 The Community and Public Sector Union (CPSU) and CLA supported the development and implementation of information-handling policies, but remained concerned about the potential for agencies to impose secrecy requirements in addition to those imposed by secrecy provisions as a part of their information-handling policies.[40] As expressed by the CPSU:

> Allowing an agency to make Commonwealth information not otherwise subject to secrecy provisions nonetheless secret by operation of agency policy and the requirement of APS employees to follow such policies is contrary to the principle of open and accountable government. All agency information handling policies should be reviewed and audited to ensure they conform to the necessary legislative standards and the Federal Government's stated position on openness in government.[41]

14.40 A similar position was taken by the Public Interest Advocacy Centre in its submission in response to IP 34, which commented 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.[42]

Transparency

14.41 CLA expressed 'strong support' for Australian Government agencies making their information-handling policies publicly available, other than in exceptional cases:

> Promoting a culture of openness requires that those who handle protected information know and understand the philosophy of open and accessible government, transparency and accountability, the application of secrecy laws and the interoperation of FOI. The agency policies on information handling and disclosure should be known and understood not just by those who handle protected information, but by the public.

---

38 Ibid, Proposal 15–2.

39 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

40 Community and Public Sector Union, *Submission SR 57,* 7 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

41 Community and Public Sector Union, *Submission SR 57,* 7 August 2009.

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

> The policies should be made public, reviewed with public input, and then regularly re-assessed on a three-to-five year review cycle.[43]

14.42 Other stakeholders that commented on this proposal also expressed support.[44] The Australian Press Council agreed that 'where guidelines are issued to public officers to help them make appropriate assessments as to secrecy, those same guidelines should be available to the public'.[45]

ALRC's views

Clarifying the application of relevant secrecy laws

14.43 Agency information-handling policies, including detailed guidelines, play an integral role in clarifying the application of secrecy laws and other information-handling obligations for Commonwealth officers and others who handle Commonwealth information. In the ALRC's view, a baseline amount of information must be included in order for information-handling policies to perform this role. In particular, policies should clearly set out:

- the types of information that an employee can lawfully disclose in the performance of his or her duties;
- the types of information for which an employee must obtain authority for disclosure;
- the circumstances in which the unauthorised handling of information could result in disciplinary action; and
- the circumstances in which the unauthorised handling of information could lead to criminal proceedings.

14.44 'Types' of information in this context could include, for example, a particular kind of information—such as personal or security classified information—or information collected for a particular purpose—such as to administer a particular Act.

14.45 In Chapters 12 and 15, respectively, the ALRC recommends that agency information-handling policies should clarify the manner in which an agency will apply administrative penalties for breaches of secrecy provisions[46] and the avenues available to Commonwealth officers to raise queries or concerns.[47]

---

43 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

44 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

45 Australian Press Council, *Submission SR 62,* 12 August 2009.

46 Recommendation 12–4.

47 Recommendation 15–3.

14.46 Agency policies along these lines can help foster effective information-handling practices by Commonwealth officers and others in a number of ways. First, they give an unambiguous guide to 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 sanctions and administrative 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.

14.47 If agency information-handling policies are drafted appropriately, the level of secrecy imposed under the policy will normally be consistent with that set out in related Commonwealth secrecy laws. However, in certain circumstances, a narrower construction may be justified on the basis of other legal requirements, such as the release of accurate information and the apolitical conduct of employees. In these circumstances, the agency should clearly set out the objectives upon which it relies to justify the discrepancy.

14.48 The ALRC agrees with the CPSU about the imperative of independent oversight of agency policies and guidelines. This is especially important in light of the possibility that the level of secrecy set out in these policies may differ—or appear to differ—from legislative secrecy requirements. In Chapter 15, the ALRC discusses the role of the proposed Information Commissioner in overseeing the application and enforcement by Australian Government agencies of secrecy obligations. In the ALRC's view, it would be consistent with this role for the proposed Commissioner to review and monitor the information-handling policies of agencies.[48]

Transparency

14.49 Save in exceptional circumstances, Australian Government agencies should publish their information-handling policies. 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.

14.50 Making Australian Government information-handling policies publicly available is consistent with the objective in the *Freedom of Information Act 1982* (Cth) 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.[49]

---

48 Recommendation 15–4.

49 *Freedom of Information Act 1982* (Cth) s 3(1)(a).

14.51 The need for public availability of government information is stressed even more strongly in the revised objects clause of 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.[50]

14.52 In the ALRC's view, the vast majority of Australian Government information-handling policies should be publicly available. However, there may be 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 national security functions. The ALRC recommends an exception from the general requirement of public release of information-handling protocols where such release would be 'unreasonable or impractical'.

14.53 In Chapter 15, the ALRC recommends a role for the proposed Information Commissioner in reviewing, and reporting to the responsible Minister on, the information-handling policies developed by agencies.[51] In that context, the Information Commissioner may provide advice on the circumstances in which it may not be reasonable for a policy, or part of a policy, to be published.

Recommendation 14–1 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;

---

50 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 1 cl 3.

51 Recommendation 15–4.

(c) the circumstances in which the unauthorised handling of information could lead to disciplinary action; and

(d) the circumstances in which the unauthorised handling of information could lead to criminal prosecution.

Recommendation 14–2 Australian Government agencies should make their information-handling policies publicly available, save in certain exceptional cases where this would be unreasonable or impractical.

Lawful and reasonable employer directions

14.54 All employees, including Commonwealth employees, must comply with any 'lawful and reasonable direction' issued by their employer. The scope of the common law duty to comply with lawful and reasonable directions is discussed in Chapter 12. 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'.[52] In the context of the public service, a somewhat broader test for the lawfulness of directions is likely to apply. [53]

14.55 The capacity to issue directions to staff can play an important role in establishing a comprehensive administrative information-handling framework. For example, in Chapter 6 the ALRC considers the regulation of unauthorised access to Commonwealth information and expresses the view that, in most circumstances, this does not warrant criminal sanctions and accordingly should not be an element of the recommended general secrecy offence. However, Australian Government agencies that hold large databases of sensitive information could issue a direction to staff prohibiting inappropriate 'browsing'. This would operate in addition to other administrative secrecy requirements, for example, in reg 2.1 of the *Public Service Regulations*.

14.56 In this Inquiry, the ALRC heard concerns about the relationship between an agency's information-handling policy and 'lawful and reasonable directions' to employees.[54] In the 1994 judgment of the Federal Court in *Phillips v Secretary, Department of Immigration and Ethnic Affairs*, Wilcox J considered whether an administrative policy amounted to an 'instruction', compliance with which was required under the *Public Service Regulations 1935* (Cth) (the predecessor to the

52 *R v Darling Island Stevedoring & Lighterage Co Ltd; Ex parte Halliday* (1938) 60 CLR 601, 621–622.

53 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.

54 See, eg, Public Interest Advocacy Centre Ltd, *Submission SR 38,* 9 March 2009, which noted the need for clarification in this regard.

current *Public Service Regulations*).[55] Despite the fact that the document was expressed to be an 'instruction', Wilcox J found its general context to be the provision of advice to officers on how they should comply with obligations sourced elsewhere. He stated that:

> A breach of [the *Public Service Regulations*] is not a criminal offence, but it exposes an officer to the sanction of dismissal. This sanction may be more severe than many criminal penalties. It seems to me that, in such a situation, the word 'instruction' … should be confined to such commands as are unequivocally intended to create new legal obligation.[56]

14.57 On the basis of this reasoning, information-handling policies and guidelines would be unlikely, without more, to be interpreted as legally binding instructions—that is, 'lawful and reasonable directions'.

14.58 In response to IP 34, Whistleblowers Australia advised 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 the secrecy directions that can be given by an agency head.[57]

14.59 In *Bennett v President, Human Rights and Equal Opportunity Commission*, 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.[58] 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.[59]

14.60 In DP 74, the ALRC proposed that Australian Government agencies should review administrative secrecy requirements that differ from reg 2.1 of the *Public Service Regulations*, including 'lawful and reasonable directions' issued to employees, to ensure that these are consistent with the implied constitutional freedom of political communication.[60] Those stakeholders that commented on this proposal expressed

---

55 Under reg 8A of the *Public Service Regulations 1935* (Cth), officers were required to comply with 'any enactments, regulations, determinations, awards or departmental instructions applicable to the performance of his or her duties'.

56 *Phillips v Secretary, Department of Immigration and Ethnic Affairs* (1994) 48 FCR 57, 81.

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

58 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 134 FCR 334. The implied constitutional freedom of political communication is discussed in Ch 2.

59 Ibid, [121].

60 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009) Proposal 14–5.

support.[61] Whistleblowers Australia suggested that a statutory provision should be enacted providing that lawful and reasonable directions must comply with the implied constitutional freedom.[62]

ALRC's views

14.61 A focus of the ALRC's recommendations in this and the preceding chapter is on establishing a consistent and effective administrative secrecy framework in the Australian Government. In particular, the ALRC recommends that equivalent secrecy obligations to those set out in reg 2.1 of the *Public Service Regulations* should apply to all Commonwealth employees, except where differences are necessary to accommodate an employing agency's specific functions or structure.[63] Above, the ALRC recommends that Australian Government agencies should develop and implement information-handling policies that clarify the application of these obligations in the particular context of their information holdings.[64] This combination provides a sufficiently nuanced secrecy framework to accommodate most information handling by Commonwealth employees.

14.62 However, as noted above, there may be situations where the potential consequences of the disclosure of Commonwealth information justify an agency giving directions to its employees over and above the standard conduct requirements. In this context, one of the limits on an agency's discretion is the relationship between the direction and the implied constitutional freedom of political communication.

14.63 The ALRC recommends that Australian Government agencies that have issued 'lawful and reasonable' secrecy directions to employees, should review these requirements for consistency with the implied constitutional freedom of political communication. Consistently with Recommendation 15–4, the proposed Information Commissioner could play a role in overseeing agency reviews.

14.64 In the ALRC's view, it is unnecessary for the *Public Service Act 1999* (Cth) or other legislation to provide that directions to employees must comply with the implied constitutional freedom of political communication. As a constitutional requirement, this restriction will apply regardless of any additional statutory expression.

---

61 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

62 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.

63 Recommendation 13–1.

64 Recommendation 14–1.

Recommendation 14–3 Australian Government agencies should review 'lawful and reasonable' secrecy directions issued to employees to ensure that these are consistent with the implied constitutional freedom of political communication.

Memorandums of understanding

14.65 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.

14.66 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 between Australian Government 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 the exchange of information among government agencies by 'formalis[ing] the terms of a relationship or framework for cooperation between the parties'.[65]

14.67 Several Australian Government agencies have MOUs in place 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'.[66] Each agency agrees, on request, to provide certain information to the other in a timely manner.[67] 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.[68] Commonwealth, state and territory police also have in place a detailed MOU for the sharing of law enforcement information.[69]

---

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

66 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> at 4 December 2009, cl 4.1.

67 Ibid, cl 4.2.

68 Ibid, cl 4.3.

69 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*.

14.68 The Community and Disability Services Ministers' Advisory Council informed the ALRC of the development of an Information Sharing Protocol between Australian Government agencies and child protection agencies. This protocol was developed in response to concerns that decisions about information sharing were 'largely subjective and open to interpretation by individual officers', which could not only result in inconsistent application, but also limit the information disclosed to child protection agencies because of a culture of risk aversion.[70]

14.69 Australian Government agencies may also enter into MOUs with foreign government agencies as regards the exchange of information. For example, ASIC has entered into an MOU with the United States Securities Exchange Commission concerning the exchange of information related to the enforcement of securities laws. The MOU recognises the 'importance and desirability of exchanging assistance and information' for the purpose of enforcing and securing compliance with securities laws. It allows, however, for a request for assistance to be denied in certain circumstances including, for example, where it would require the authority to act in a manner that would violate its domestic law. The MOU also imposes conditions on the use to which information provided under it can be put by the requesting partner.[71]

Submissions and consultations

14.70 In submissions in response to IP 34, several stakeholders noted the effectiveness of MOUs in protecting Commonwealth information. For example, the Australian Government Attorney-General Department (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'.[72] The ATO agreed that MOUs were 'an effective tool for setting up protocols for the exchange of information with other agencies'.[73]

14.71 In DP 74, the ALRC proposed 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.[74]

---

70 Community and Disability Services Ministers' Advisory Council, *Submission SR 80,* 28 August 2009.

71 United States Securities and Exchange Commission and Australian Securities and Investments Commission, *Memorandum of Understanding Concerning Consultation, Cooperation and the Exchange of Information Related to the Enforcement of Securities Laws*, 25 August 2008.

72 Attorney-General's Department, *Submission SR 36,* 6 March 2009. See also Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.

73 Australian Taxation Office, *Submission SR 13,* 16 February 2009. See also Commonwealth Ombudsman, *Submission SR 20,* 19 February 2009.

74 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 15–3.

14.72 Stakeholders generally agreed that MOUs would facilitate the mutual exchange of information.[75] The ATO advised that it has in place a number of MOUs with other Australian Government agencies with which it shares information, as well as state and territory revenue offices. These 'are an effective tool for setting up protocols for the exchange of information, and therefore can assist staff in complying with their secrecy obligations'.[76] In response to another of the ALRC's proposals, the Australian Transaction Reports and Analysis Centre (AUSTRAC) commented that 'MOUs are important in establishing the expectations of the parties in respect of the exchange of information'.[77] The Social Security Appeals Tribunal also noted that MOUs it has in place with Centrelink and the Child Support Agency facilitate the mutual exchange of information.[78]

14.73 Despite the broad support for this proposal, some concerns were raised about the lack of transparency of many MOUs. For example, although Whistleblowers Australia agreed that MOUs may be helpful in the management of information, it commented that these are 'private arrangements' and 'therefore they provide another example of the process of concealment that is not transparent'.[79] The Australian Privacy Foundation also expressed the view that MOUs should be made publicly available.[80]

14.74 The Department of Immigration and Citizenship (DIAC) suggested that, in the absence of a standard MOU, the use of MOUs to regulate information sharing between Australian Government agencies may result in an inconsistent approach to the way that information is shared between agencies.[81]

ALRC's views

14.75 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, including foreign partners. In particular, MOUs formalise the standard information-sharing protocols between agencies and others. 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

---

75 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

76 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

77 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009. In AUSTRAC's view, these must be underpinned by specific secrecy provisions that regulate the disclosure of information. See also Australian Transaction Reports and Analysis Centre, *Submission SR 31,* 2 March 2009.

78 Social Security Appeals Tribunal, *Submission SR 79,* 24 August 2009.

79 Whistleblowers Australia, *Submission SR 74,* 17 August 2009. See also Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009.

80 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

81 Department of Immigration and Citizenship, *Submission SR 59,* 7 August 2009.

information by creating certainty in the information-sharing framework. Where a disclosure is validly authorised under an MOU, it is likely to indicate that the disclosure will fall within exceptions in criminal and administrative secrecy provisions for disclosures in the course of an employee's functions or duties. In the ALRC's view, 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.

14.76 The ALRC agrees with the view of Whistleblowers Australia and others that these MOUs should be made publicly available in order to ensure transparency and accountability in information-sharing arrangements. This reasoning and approach is consistent with the Report, *Principled Regulation: Federal Civil and Administrative Penalties in Australia*, where the ALRC recommended that regulators who administer legislation under which criminal penalties may be imposed should, together with the Commonwealth Director of Public Prosecutions (CDPP), develop and publish MOUs detailing the use of non-criminal penalties and their relationship with criminal referrals to the CDPP.[82] Publishing information-sharing MOUs will also address DIAC's concerns about the potential for inconsistency in information sharing by facilitating access to a range of agreements, which agencies can amend to suit their particular information holdings and sharing needs. In the ALRC's view, this provides a more nuanced response than, say, the development of a uniform agreement.

14.77 Above, the ALRC recommends that Australian Government agencies should make their information-handling policies publicly available.[83] The ALRC recognises, however, that, in a small number of situations, publication of this information may be unreasonable or impractical—for example, where public knowledge about the pattern of information sharing between intelligence agencies could impede national security. The ALRC recommends an equivalent exception in the context of the public availability of MOUs.

Recommendation 14–4 Australian Government agencies that regularly share information with other agencies or bodies should enter into memorandums of understanding (MOUs) setting out the terms and conditions for the exchange of information. Australian Government agencies should make such MOUs publicly available save in certain exceptional cases where this would be unreasonable or impractical.

82 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 9–1.

83 Recommendation 14–2.

Information and communication technology systems

14.78 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.[84]

Protecting Commonwealth information

14.79 ICT systems, such as access controls, can lessen the opportunity for inadvertent or deliberate non-compliance with information-handling guidelines and policies 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.[85] 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.

14.80 In its 2009 Audit Report, *Interim Phase of the Audit of Financial Statements of General Government Sector Agencies for the Year Ending 30 June 2009*, the ANAO advised that information technology security controls implemented by Australian Government agencies had improved significantly over the preceding 12 months.[86] The ANAO advised that:

> In 2007–08, almost a third of agencies did not have a current and management endorsed security governance structure in place. This year almost all agencies had established effective security governance controls.
>
> Similarly, agencies have improved their network security procedures to provide authorised access and control of remote access information flows. The ANAO found this year that, in general, agencies have also improved their security awareness and training practices and procedures.[87]

14.81 There were some agencies, however, that still had significant security risks associated with their ICT systems.[88]

---

84 Australian Public Service Commission, *State of the Service Report 2006–07* (2007), 241.
85 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.
86 Australian National Audit Office, *Interim Phase of the Audit of Financial* (2009), 67.
87 Ibid, 67–68.
88 Ibid, 200–201.

Sharing Commonwealth information

14.82 Effective ICT systems may also promote information-sharing by standardising information-handling practices that may otherwise be contentious or dependent on the exercise of individual discretion. By way of illustration, CrimTrac's National Criminal Investigation DNA Database (NCIDD) provides police with access 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.[89]

14.83 In another context, the Secrecy and Disclosure Project, within the Serious Non Compliance branch of the ATO, is developing a streamlined system to manage the disclosure of protected tax information to law enforcement agencies and Project Wickenby partners.[90] This includes, for example, the creation of specific 'information packages', reflecting the information requested and its intended use; automatic reduction of sensitive material and watermarking where required; and secure, electronic dissemination of the approved information packages to the requesting agency.[91]

14.84 The use of ICT systems to foster whole of government activities and promote the principles of open government is receiving ongoing attention from the Australian Government. Several Australian Government-wide ICT strategies have been implemented to promote secure information sharing including FedLink, a whole of government encryption system, and GovDex, a web-based space for secure information sharing. Broader changes in the management of ICT at the Australian Government level are being considered in response to the recommendations of the *Review of the Australian Government's Use of Information and Communication Technology*, led by Sir Peter Gershon (the Gershon review).

14.85 The report of the Gershon review was released in October 2008, and reported 'ad hoc, reactive and siloed responses' to ICT in Australian Government agencies,[92] which was hindering the ability of the Australian Government to 'provide efficient and effective joined-up ICT-enabled services to citizens and businesses'.[93] The review made wide-ranging recommendations for reform, including the establishment of a ministerial council on ICT with responsibility for ICT policies and whole of

89 CrimTrac, *Annual Report 2006–07* (2007), 18–21.

90 Project Wickenby is a multi-agency taskforce led by the ATO to investigate tax avoidance, tax evasion and large-scale money laundering.

91 D Boucher, *Report of a Review of Information Handling Practices in the Serious Non Compliance Business Line of the Australian Taxation Office* (2008), [119].

92 P Gershon, *Review of the Australian Government's Use of Information and Communication Technology* (2008), [4.1].

93 Ibid, [4.1].

government ICT[94] and a requirement for agencies to seek approval from the ministerial council to opt out of whole of government ICT arrangements.[95] In November 2008, the Australian Government endorsed the recommendations of the Gershon review in full and initiated the ICT Reform Program.[96]

14.86 Significant changes to the use of ICT systems to share information within and between agencies and, in particular, with members of the public are also likely to arise out of the recommendations of the Government 2.0 Taskforce, discussed in Chapter 2.

Submissions and consultations

14.87 In IP 34, the ALRC asked about the effectiveness of Australian Government ICT systems in protecting Commonwealth information.[97] 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.[98] The Australian Federal Police noted that it has located reminders about secrecy requirements throughout its intranet where sensitive information is stored.[99]

14.88 Australian Government agencies in other areas also made submissions about how they use ICT systems to protect their information. The Australian Bureau of Statistics (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.[100] The AGD also advised that it had the capacity to 'lock down' information to certain persons on a need-to-know basis.[101]

14.89 In DP 74, the ALRC recognised the potential for ICT strategies to assist Commonwealth employees and others to comply with their obligations of secrecy and other information-handling responsibilities. The ALRC proposed that Australian Government agencies should implement ICT systems to facilitate the secure and convenient handling of Commonwealth information, including access controls and

94 Ibid, [5.1.1].
95 Ibid, [5.1.3].
96 Department of Finance and Deregulation, *Review of the Australian Government's Use of Information and Communication Technology* (2009) <www.finance.gov.au/publications/ICT-Review/index.html> at 20 November 2009.
97 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 6–3(c).
98 Australian Transaction Reports and Analysis Centre, *Submission SR 31,* 2 March 2009.
99 Australian Federal Police, *Submission SR 33,* 3 March 2009.
100 Australian Bureau of Statistics, *Submission SR 28,* 24 March 2009.
101 Attorney-General's Department, *Submission SR 36,* 6 March 2009.

audit mechanisms.[102] The ALRC did not make a proposal about the use of ICT systems to promote information sharing.

14.90 Stakeholders that commented on this proposal were unanimously supportive.[103] The ATO, for example, advised that it has a strong information technology security culture, including a practice statement applicable to staff, contractors and service providers about the protection and security of the ATO's ICT systems. The ATO further submitted that it regularly audits its ICT systems to ensure ongoing confidentiality, integrity and accessibility of its data.[104]

ALRC's views

14.91 A diverse array of ICT strategies are 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.

14.92 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 recommends that Australian Government agencies should implement protective ICT systems—in particular, access controls and audit mechanisms.

14.93 The ALRC is not making a recommendation about the use of ICT systems to promote information sharing. This issue was comprehensively considered in the Gershon review, the recommendations of which the Australian Government is in the process of implementing. These issues will receive further attention by the Government 2.0 Taskforce.[105]

Recommendation 14–5 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.

---

102 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 15–6.

103 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

104 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

105 Government 2.0 Taskforce, *Towards Government 2.0: An Issues Paper* (2009).

Data matching

14.94 Data matching has been described by the 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'.[106] 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.[107]

14.95 In a submission to this Inquiry, the Australian Commission for Law Enforcement Integrity said that '[a]s in many other areas of government, collecting, analysing and sharing information is at the heart of law enforcement activity':[108]

> 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.[109]

14.96 However, data-matching is also associated with privacy risks and community concern. As noted by the Privacy Commissioner, data matching may involve the:

- use of personal information for purposes other than the reasons it was collected—which may not be within the reasonable expectations of the individuals to whom the information relates;
- examination of personal information where there are no grounds for suspicion, sometimes without the knowledge of the individuals to whom the information relates; and
- retention of matched information by agencies for potential future use.[110]

---

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

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

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

109 Ibid.

Legislative framework

14.97 Agencies wishing to undertake data-matching activities must comply with a number of laws including the *Privacy Act 1988* (Cth), *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and secrecy provisions.

Privacy Act

14.98 As discussed in Chapter 16, the *Privacy Act* imposes obligations on Australian Government agencies and private-sector organisations (as defined in that Act) in relation to the handling of personal information, which may impact on data-matching activities. For example, under Information Privacy Principle (IPP) 10, an agency may only use personal information for a purpose other than the primary purpose of collection where one of the specified requirements has been met—for example, where the individual has consented or the use is reasonably necessary for the purpose of law enforcement.[111] Similar requirements apply to disclosure of information under IPP 11.[112]

Data-matching Program (Assistance and Tax) Act

14.99 The *Data-matching Program (Assistance and Tax) Act* and related guidelines regulate the use of tax file numbers to match data held by certain agencies, such as the ATO and Centrelink. The Privacy Commissioner monitors, and has powers to enforce, compliance with the Act and the Guidelines. However, the *Data-matching Program (Assistance and Tax) Act* and Guidelines only apply to a limited subset of data-matching activities.

14.100 The Privacy Commissioner has issued voluntary guidelines for agencies that engage in other data-matching practices, which aim to ensure that these programs 'are designed and conducted in accordance with sound privacy practices'.[113] Although the guidelines are not legally binding, a number of agencies have agreed to comply with them.[114] In summary, the voluntary 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.[115]

---

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

111 *Privacy Act 1988* (Cth) s 14 IPP 10.

112 Ibid s 14 IPP 11.

113 The voluntary data-matching guidelines apply to agencies that match data from two or more databases, if at least two of the databases contain information about more than 5,000 individuals.

114 See discussion in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Ch 10.

115 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998), [33]–[47], [63], [69]. In Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), the ALRC suggested that the

14.101 The ALRC considered the application of these laws and guidelines in the 2008 Report, *For Your Information: Australian Privacy Law and Practice* (ALRC 108), including whether there was a need for the data-matching programs that fall outside the *Data-matching Program (Assistance and Tax) Act* to be regulated more formally.[116] The ALRC did not consider that a case had been made out for making these guidelines mandatory. Rather, the ALRC suggested that the Office of the Privacy Commissioner could exercise its function of researching and monitoring technology to review the adequacy of, and compliance with, the existing guidelines if it deemed this to be necessary.[117]

Secrecy provisions

14.102 Unless a relevant exception applies, secrecy provisions may prevent the disclosure of Commonwealth information for the purpose of data matching. The impact of a secrecy provision on potential data-matching activities will be most acute where the provision regulates a broad category of information in the absence of an express harm requirement. Any exceptions or defences that are available will also be relevant.

14.103 In the 1995 inquiry into the protection of confidential personal and commercial information held by government 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.[118]

Submissions and consultations

14.104 In IP 34, the ALRC asked about any concerns arising from the interaction between secrecy provisions and data-matching laws and practices.[119] Liberty Victoria warned 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

---

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.

116 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Ch 10.

117 Ibid, [10.97]–[10.99].

118 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.

119 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 7–6.

> correctly, data matching and secrecy provisions should work together to ensure only necessary data matching is undertaken with appropriate safeguards.[120]

14.105 The importance of robust controls was echoed by AUSTRAC, which 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 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.[121]

14.106 The Office of the Privacy Commissioner expressed the view that 'data matching activities should continue to be limited to very specific needs and purposes and be subject to clear guidance about how the activities are undertaken'. The Office noted that agencies that wish to undertake data matching must first determine whether information they hold can be released pursuant to their secrecy provisions. Should this be the case, the agency must consider its obligations under the *Privacy Act*:

> The Office supports the ability to share information within and between governments and the private sector where a clear and legitimate purpose is identified. While data matching can be a very useful tool for a wide variety of purposes, it has the potential to significantly change the way that personal information is handled. This includes such risks as a change in the nature of the information, once combined, becoming more sensitive, as well as the context within which it was originally held becoming vastly different. Similarly, data matching may result in information being used in a way that is beyond the normal expectation of an individual.[122]

14.107 The Office submitted that to date, the interaction of secrecy provisions and the *Privacy Act* has provided satisfactory protection. However, to ensure appropriate protection in the context of future technological advances, it suggested that the ALRC consider making the voluntary public sector data matching guidelines mandatory.[123]

14.108 In DP 74, the ALRC expressed the preliminary view that current legislation and policies, in addition to reforms proposed elsewhere in the Discussion Paper, provided an appropriate framework for data-matching activities in the Australian Government. In particular, the ALRC considered that the proposed exception to the

---

120 Liberty Victoria, *Submission SR 19,* 18 February 2009.
121 Australian Transaction Reports and Analysis Centre, *Submission SR 31,* 2 March 2009.
122 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009.
123 Ibid.

general secrecy offence, and other specific secrecy offences, for disclosures authorised by the relevant agency head or minister could facilitate data-matching in appropriate cases.[124]

14.109 The AGD agreed with an approach of authorising information-sharing activities, including data matching, through agency level agreements. It noted that these agreements should fit within a broader information-management framework.[125]

14.110 The Office of the Privacy Commissioner noted the ALRC's view that information sharing could best be undertaken through individual agency agreements as part of a broader information-management framework. However, it suggested that these agreements should include a requirement for data-matching activities involving significant volumes of data to be subject to guidelines issued by the Privacy Commissioner. The Office reiterated its view that the ALRC should consider recommending that the voluntary data-matching guidelines be mandatory for the public sector.[126] A similar argument was put forward by the Australian Privacy Foundation, which submitted that the ALRC should recommend compliance with data-matching guidelines, along with the use of Privacy Impact Assessments (PIAs), in the context of information-sharing arrangements.[127]

14.111 The ABS focused on the importance of secrecy provisions enabling Australian Government agencies to disclose information to the ABS for statistical data matching.[128]

ALRC's views

14.112 As a general principle, information sharing between government agencies, and government and the private sector—including data matching—should be undertaken at the agency level through individual agency agreements. These agreements should be clearly situated within a broader information-handling framework, including the *Privacy Act*, data-matching guidelines and legislation, and any applicable secrecy provisions. In the ALRC's view, this framework suitably accommodates the tension between the need for secrecy and openness inherent in data matching.

14.113 The ALRC is not recommending that the voluntary data-matching guidelines should be made mandatory. This issue was considered in ALRC 108, where the ALRC noted that there was a lack of evidence that agencies were failing to comply with the voluntary guidelines. Accordingly, the ALRC did not consider that a case had been

---

124 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Ch 3.
125 Attorney-General's Department, *Submission SR 67,* 14 August 2009.
126 Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009.
127 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009. PIAs are discussed in Ch 16, and were the subject of several recommendations in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008).
128 Australian Bureau of Statistics, *Submission SR 58,* 7 August 2009.

made out for making these guidelines mandatory. The ALRC suggested, and remains of the view that, the Office of the Privacy Commissioner could exercise its function of researching and monitoring technology to review the adequacy of, and compliance with, the existing guidelines if it deemed this to be necessary.[129]

14.114 Another regulatory option that may be available in the context of large-scale data-matching programs is a PIA. As discussed in Chapter 16, the ALRC has previously recommended that the Privacy Commissioner should be empowered to direct an agency to provide a PIA in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[130] The Australian Government has accepted this recommendation.[131] This is likely to include, for example, data-matching activities involving significant volumes of data.

129 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [10.97]–[10.99].

130 Ibid, Rec 47–4.

131 Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

15. A Culture of Effective Information Handling

Contents

Introduction

15.1 Cultural change is an important factor in driving reforms, including a shift in emphasis from a much criticised 'culture of secrecy'[1] towards principles of open government. As one stakeholder commented in the context of the introduction of Government 2.0:

> Leadership from the highest levels and generational change is required to make this a reality. The key is not to expect too much too soon as transparency is a terrifying concept for most government agencies and their officers.
>
> All of the technical, legal and logistical problems will be solvable, but worthless without real cultural change at all levels of government.[2]

15.2 This chapter focuses on strategies for promoting an effective information-handling culture among Australian Government agencies and their employees. An effective information-handling culture minimises the unauthorised handling of

---

1 See comments in 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 Government 2.0 Taskforce, *Towards Government 2.0: An Issues Paper* (2009), 13. The Government 2.0 Taskforce is discussed in Ch 2.

Commonwealth information while encouraging information sharing in appropriate circumstances.

15.3 The first section of this chapter examines the various risk factors that may lead to inappropriate information sharing and a number of strategies that may overcome these risks. In particular, the ALRC considers the role of senior employees and supervisors, training and development programs, oaths and affirmations of secrecy and avenues for employees to ask questions and raise concerns. Clear and well-disseminated information-handling policies and effective information and communication technology (ICT) platforms, as recommended in Chapter 14, will also assist in promoting compliance with information-handling responsibilities.

15.4 The chapter goes on to consider strategies to promote effective information-handling culture at the level of Australian Government agencies—in particular, by recommending a role for the proposed Information Commissioner.[3]

Individual Commonwealth employees

Risk factors

15.5 The Queensland Crime and Misconduct Commission (CMC) has identified a number of risk factors that are associated with the misuse of official information, including intentional non-compliance—that is, the deliberate 'leaking' or inappropriate withholding of Commonwealth information—and unintentional non-compliance.

15.6 The CMC notes that, among other factors, the *deliberate* release of information may be motivated by:

- personal motivations, such as the desire or need to sell information for profit or personal advantage, dissatisfaction with the stifling of debate, or lack of recognition for the officer's individual or professional views;
- 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.[4]

---

3 As discussed below, establishment of an Information Commissioner for the Australian Government is the subject of the Exposure Draft, Information Commissioner Bill 2009 (Cth).

4 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 made, for example, in P Durbin, 'ATO lashed over privacy breaches', *Australian Financial Review*, 23 April 2009, 1.

15.7 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.[5]

15.8 Similar issues may contribute to an inappropriate failure to share information. For example, personal motivations may result in a Commonwealth officer deliberately withholding information where disclosure could reveal misconduct. 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 disclosing information that could properly be shared—or a lengthy delay before such sharing occurs.

15.9 Qualitative research into organisational misconduct more broadly has identified the importance of organisational factors, as compared with personal characteristics, as potential precursors of misconduct. For example, a survey of employees in for-profit, non-profit and government organisations reported that formal organisational compliance practices—such as written codes and ethics training—and the informal ethical climate—such as leaders setting a good example—were independent predictors of employee conduct. The authors noted the importance of 'promoting a moral organization through the words and actions of senior managers and supervisors, independent of formal mechanisms such as codes of conduct'.[6] The *Deloitte & Touche USA 2007 Ethics and Workplace Survey* reported that respondents viewed the role of managers and direct supervisors as being the strongest influences on ethical behaviour at work. In comparison, only 10% of respondents cited criminal penalties for violation of a code of conduct as a factor that helped foster an ethical workplace.[7]

Leadership from senior employees and supervisors

15.10 As noted above, the example set by senior employees and direct supervisors is a strong influence on employee conduct, capable of predicting misconduct independently of formal organisational compliance mechanisms such as codes of conduct. Leadership from these staff is crucial for fostering a culture of effective information handling.

---

5 Crime and Misconduct Commission Queensland, *Information Security—Keeping Sensitive Information Confidential*, Building Capacity Series Number 7 (2005), 5.

6 N Andreoli and J Lefkowitz, 'Individual and Organizational Antecedents of Misconduct in Organizations' (2009) 85 *Journal of Business Ethics* 309, 309.

7 Deloitte, *Leadership Counts: Deloitte & Touche USA 2007 Ethics and Workplace Survey* (2007) <www.deloitte.com> at 27 July 2009.

15.11 Several provisions of the *Public Service Act 1999* (Cth) impose requirements to promote the Australian Public Service (APS) Values and Code of Conduct, including the administrative secrecy provision in reg 2.1 of the *Public Service Regulations 1999* (Cth).[8] Section 35 of the Act sets out the constitution and role of the Senior Executive Service (SES), including that each member of the SES must promote 'by personal example and other appropriate means' the APS Values and compliance with the Code of Conduct.[9] Section 12 requires agency heads to 'uphold and promote the APS Values'.

15.12 The influence of supervisors in establishing an agency's information-handling culture was recognised by the ALRC and the Administrative Review Council (ARC) in their 1995 review of the *Freedom of Information Act 1982* (Cth) (ALRC 77). The ALRC and ARC recommended that the performance agreements of all senior officers[10] should include a responsibility to ensure efficient and effective practices and performance in respect of access to information, including freedom of information (FOI) requests.[11]

ALRC's views

15.13 The ALRC continues to see the benefits of including in the performance agreements of senior officers in Australian Government agencies a responsibility to ensure efficient and effective information-handling practices. As noted in ALRC 77, giving tangible incentives to staff to pay greater attention to, and to improve, an agency's information-handling practices will increase the likelihood of cultural change.[12] This will supplement relevant obligations in the *Public Service Act*, identified above.

15.14 As discussed below, training and development programs will be an important strategy for improving the information-handling example set by senior employees and supervisors.

Training and development programs

15.15 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.[13]

---

8 The requirements of reg 2.1 are discussed in detail in Ch 12, as well as recommendations for reform.

9 *Public Service Act 1999* (Cth) s 35(2)(c).

10 'Senior officer' was defined in that report as all SES officers and Senior Officers Grades A to C. The classification system has been amended since that time. The general classification levels next most senior to the SES are Executive Level 1 and 2: *Public Service Classification Rules 2000* (Cth).

11 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 8.

12 Ibid, [4.16].

13 Sometimes training and development can also be used as an administrative action to address breaches of secrecy laws.

15.16 In its *State of the Service Report 2001–02*, the Australian Public Service Commission (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).[14]

15.17 The APSC noted that although the majority of employees are informed of their obligations in relation to handling Commonwealth information when they commence employment, 42% of agencies did not provide employees with regular reminders of these obligations.[15]

15.18 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 operation of the *Freedom of Information Act 1982* (Cth) (FOI Act); advises on the application of privacy and secrecy laws; and provides contact officers to approach for further information.[16]

15.19 The Commonwealth Ombudsman, in reviewing the collection, storage and dissemination of information in the Australian Crime Commission (ACC), commented that the ACC's induction program provided 'a good introduction to security practices and, in particular, physical and document security and document security classification and handling'. The Ombudsman suggested, however, that the induction could be enhanced by:

- explaining the s 51 secrecy provision
- describing the need-to-share and need-to-know continuum, and expounding the ACC's policy position on this
- explaining access-control measures for database documents
- explaining the role of the IT Security Adviser

---

14 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.

15 Ibid.

16 Centrelink, *Centrelink Graduate and Cadet Induction: Confidentiality, Privacy, Freedom of Information* (2009).

- describing and defining information misuse and information access breaches, and the sanctions
- providing a more defined incident reporting process for suspected ICT and information security breaches.[17]

15.20 In February 2009, the ALRC conducted an open forum about secrecy laws with members of the Community and Public Sector Union (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 relevant, employees go 'straight to a fear culture'.[18] Callers to the ALRC's secrecy phone-in also raised issues about training and development programs, including the need for Commonwealth employees to be trained about broader ethics and values in relation to government information handling, in order to instil a greater culture of transparency.

Submissions and consultations

15.21 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC noted the importance of training and development programs in fostering compliance by employees and others with information-handling regimes. The ALRC proposed that Australian Government agencies should develop and administer training and development programs for their employees on their information-handling obligations, including the need to share information in certain circumstances and avenues for making public interest disclosures.[19]

15.22 Civil Liberties Australia 'strongly supported' the proposal, noting that 'a culture of openness and accessibility can be achieved if Commonwealth officers know and understand the circumstances in which it is appropriate to share information and how to make public interest disclosures'.[20] The Australian Press Council agreed that all officials should receive adequate training in the correct implementation of any laws, regulations, guidelines or rulings relevant to the classification or declassification of confidential material.[21] Many other submissions also expressed support for training and development programs.[22]

---

17 Commonwealth Ombudsman, *Australian Crime Commission: Review of the Collection, Storage and Dissemination of Information*, Report No 15 (2009), [2.120].

18 Community and Public Sector Union Members Secrecy Forum, *Consultation*, Canberra, 3 February 2009.

19 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 15–4.

20 Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

21 Australian Press Council, *Submission SR 62,* 12 August 2009.

22 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; 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

15.23 The Department of Immigration and Citizenship (DIAC) noted that training will be especially important if a harm-based general secrecy offence is adopted, because of the degree of subjectivity in assessing whether the disclosure of information would cause harm to a specified public interest.[23]

15.24 The Australian Privacy Foundation suggested that Australian Government agencies should be under a particular obligation to provide training and development programs for FOI and privacy officers.[24]

ALRC's views

15.25 In order for employees to operate in accordance with secrecy and other information-handling obligations, they must first know the scope of these obligations and the purpose that they serve.

15.26 The ALRC recommends that Australian Government agencies develop and administer training and development programs for their employees about the information-handling obligations relevant to their position, including the need to share information in certain situations. As noted by DIAC, articulating these obligations may be especially important in the context of the harm-based secrecy framework recommended in this Report. Training and development programs should also clarify the avenues available to employees and others to raise queries or concerns about their information-handling responsibilities,[25] and to make public interest disclosures.[26]

15.27 In the ALRC's view, 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 is in the position of managing staff.

Taxation Office, *Submission SR 13,* 16 February 2009; Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.

23 Department of Immigration and Citizenship, *Submission SR 59,* 7 August 2009.

24 Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

25 Avenues for employee queries and concerns are considered below.

26 As noted throughout this Report is premised on the introduction of robust public interest disclosure legislation.

Recommendation 15–1 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 need to share information in certain situations. Programs should also provide information about how employees can raise concerns and make public interest disclosures.

Oaths, affirmations and acknowledgements of secrecy

15.28 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.[27] 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.[28] 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.[29]

15.29 Many oaths and 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 secrecy provision. 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.[30]

---

27 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.

28 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.

29 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.

30 *Income Tax Regulations 1936* (Cth) sch 1 (emphasis added).

15.30 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.[31]

15.31 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.[32]

15.32 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.[33]

15.33 Moreover, oaths and affirmations may carry considerable 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.[34]

---

31 This was a topic that arose 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.

32 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.

33 *Kessing v The Queen* [2008] NSWCCA 310, [10].

34 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

15.34 The capacity for oaths and affirmations to remind staff of their obligations of secrecy was commented on in a number of submissions on the Issues Paper, *Review of Secrecy Laws* (IP 34).[35] For example, the Department of Human Services submitted that 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.[36]

Submissions and consultations

15.35 In DP 74, the ALRC expressed the view that the relevant Australian Government agency should retain the discretion to administer an oath or affirmation of secrecy, in accordance with any legislative provision. However, the ALRC proposed that where an agency decides to administer such an oath, it should ensure that it is an accurate reflection of the requirements under relevant Commonwealth secrecy laws.[37] In particular, the ALRC was concerned about the potential for oaths and affirmations to set out broader or more onerous obligations than the secrecy laws on which they are based.

15.36 Those stakeholders who commented on this proposal were unanimously in support.[38] The Australian Taxation Office (ATO) advised that it asks new tax officers and contracted staff to sign a declaration of secrecy, with the aim of ensuring compliance with the relevant taxation secrecy provision.[39]

ALRC's views

15.37 The strong moral significance accorded to oaths and affirmations of secrecy means that they could play a valuable role in reinforcing a Commonwealth employee's responsibilities to protect official information. 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.

15.38 The ALRC remains of the view that Australian Government agencies should have the discretion to decide whether or not to administer an oath or affirmation of

---

Legislation' (1990) 19 *Federal Law Review* 49, 74, which argues that oaths of secrecy reinforce an 'atmosphere of unnecessary secrecy'.

35 See 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.

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

37 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 15–5.

38 Department of Human Services, *Submission SR 83,* 8 September 2009; Department of Health and Ageing, *Submission SR 81,* 28 August 2009; R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

39 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

secrecy, in accordance with any legislative provision. However, where an agency does administer such an oath or affirmation, the agency should ensure that it accurately reflects the requirements under relevant Commonwealth secrecy laws. In particular, the obligations in the oath or affirmation should be no more onerous than those in the secrecy provision on which it is based. This proposal received widespread support from stakeholders.

Recommendation 15–2 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.

Employee queries and concerns

15.39 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.[40] This advice will usually come from an employee's supervisor. Agencies may establish additional frameworks for an employee to raise queries or concerns about his or her obligations of secrecy.

15.40 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 employees to the ATO Legal Services Branch where they may seek further advice or assistance.[41]

15.41 Another option for dealing with queries or concerns about secrecy oligations is through a program to provide employees with ethics advice more generally. One such strategy is the APSC Ethics Advisory Service, which was launched on 6 May 2009.[42] The service provides 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.[43] In other situations, an

40 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 30 November 2009, ch 3.

41 Australian Taxation Office, *ATO Practice Statement: Secrecy and Privacy Obligations*, PS CM 2004/07 (2004), 4.

42 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <www.smos.gov.au/speeches> at 6 December 2009.

43 Ibid. See also Australian Public Service Commission, *Introducing the Ethics Advisory Service* (2009) <www.apsc.gov.au> at 6 December 2009.

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.[44]

15.42 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.

15.43 In DP 74, the ALRC proposed that Australian Government agencies should develop information-handling policies that include, among other information, avenues for an employee to raise queries or concerns.[45] The submissions on this proposal are discussed in detail in Chapter 14. As noted in that chapter, however, there was overwhelming stakeholder support for developing such policies.

ALRC's views

15.44 Providing Commonwealth employees with avenues to raise queries and explore concerns about secrecy laws may help to promote effective information handling in two ways. First, where an 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. Secondly, to the extent that a deliberate breach is motivated by an employee feeling as though his or her views have not been 'heard' by an agency, providing the employee with an avenue to raise concerns may to some extent meet this need.

15.45 The ALRC remains of the view that the information-handling policies that Australian Government agencies develop in accordance with Recommendation 14–1 should include, among other information, avenues for an employee to raise queries or concerns.

15.46 In the ALRC's view, there is no need to specify a particular system that agencies must institute. As long as a clear pathway is provided, agencies should have a broad discretion as to the manner in which they satisfy this obligation, depending, for example, on their structure and functions, and any related initiatives that they have 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.

---

44 For example, the CMC 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 CMC 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.

45 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 15–1.

15.47 The avenues for queries and concerns about secrecy laws that are developed by Australian Government agencies should be accompanied by readily accessible avenues for employees to make public interest disclosures, discussed below.

Recommendation 15–3 The information-handling policies developed by Australian Government agencies in accordance with Recommendation 14–1 should set out how employees can raise concerns about their information-handling obligations.

Public interest disclosures

15.48 A number of the risk factors for the unauthorised disclosure of information identified by the CMC are connected to a lack of authorised avenues for employees to voice concerns or grievances. For example, an employee may disclose information because he or she feels that debate is being stifled, or suspects that his or her individual or professional views have been ignored. An unauthorised disclosure could also be a reaction to perceived shortcomings in organisational culture, such as a practice of misuse or unauthorised release of information by senior management. Concerns of this kind could potentially be identified and rectified through pathways for public interest disclosures.

15.49 As noted in Chapter 2, there is minimal protection at the Commonwealth level for people who make public interest disclosures. Section 16 of the *Public Service Act* provides some limited protection for APS employees who report breaches of the APS Code of Conduct.

15.50 Some stakeholders made submissions on the importance of having available avenues for whistleblowing.[46] Dr 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.[47] 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.[48] The Australian Commission for Law Enforcement Integrity (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.[49] 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.[50]

---

46 Public interest disclosure, or 'whistleblowing', is discussed in Chs 2 and 9.
47 J Renwick, *Submission SR 02,* 11 December 2008.
48 Community and Public Sector Union, *Submission SR 32,* 2 March 2009.
49 Australian Commission for Law Enforcement Integrity, *Submission SR 18,* 18 February 2009.
50 *Secrecy Phone-In*, 11–12 February 2009.

15.51 In February 2009, the House of Representatives Standing Committee on Legal and Constitutional Affairs (the Standing Committee) issued a report on whistleblower protection for the Commonwealth public sector (the *Whistleblower Protection* report).[51] The Standing Committee recommended that the Australian Government should establish by legislation a system for employees in the Commonwealth public sector to make disclosures about serious matters to their organisation, other public service agencies or, in limited circumstances, publicly. A person who made a disclosure under the framework would be protected from detrimental action in the workplace and receive immunity from criminal and civil liability and administrative penalties.[52]

15.52 At the time of writing, the Australian Government had not responded to the *Whistleblower Protection* report, although the Government has indicated that it intends to develop public interest disclosure legislation in 2009.[53] For the purposes of this Report, the ALRC is proceeding on the basis that such legislation will be put in place and that it will largely reflect the recommendations made in the *Whistleblower Protection* report. Accordingly, the importance of processes for Commonwealth employees to make public interest disclosures is not the subject of a recommendation in this chapter. However, these processes will be an integral component of creating an effective information-handling culture within Australian Government agencies.

Australian Government agencies

15.53 A common theme of this Inquiry is the personal nature of secrecy obligations. Individual compliance, however, depends upon the practices and processes of Australian Government agencies. For example, one of the risk factors identified by the CMC for the unauthorised disclosure of information by individuals is a failure by the employing agency consistently to 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.

15.54 Just as importantly, agency culture can prevent information from being disclosed in situations where disclosure would be lawful and appropriate. As has been commented on extensively in the context of FOI, there are compelling drivers for agencies to sacrifice the goals of openness and accountability because of a real or perceived need for non-disclosure. Such a 'culture of secrecy' was criticised by the ALRC and the ARC in ALRC 77.[54] In 2008, the Independent Review Panel examining

---

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

52 Ibid, Rec 14.

53 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <www.smos.gov.au/speeches> at 6 December 2009.

54 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.

the *Freedom of Information Act 1992* (Qld) discussed the tensions 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.[55]

15.55 In its submission in response to IP 34, 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 agencies pose a greater barrier to information sharing than legislative restrictions.[56]

15.56 The final section of this chapter discusses the information-handling culture at the level of Australian Government agencies, including strategies to shift agencies towards a culture of increased openness and transparency. In particular, the ALRC discusses the role and limitations of current oversight agencies and recommends an increased role for the proposed Information Commissioner in monitoring the compliance by Australian Government agencies of secrecy laws and other information-handling responsibilities.

Oversight of information handling in the Australian Government

15.57 The roles of a number of Australian Government office-holders may encompass the oversight and monitoring of secrecy and other information-handling practices in the Australian Government, or in particular Australian Government agencies. The functions and powers of these offices are outlined below.

Commonwealth Ombudsman

15.58 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.[57] This potentially includes a range of practices regarding Commonwealth information—

---

55 Freedom of Information Review Panel, *Enhancing Open and Accountable Government*, Discussion Paper (2008), 90–91.

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

57 *Ombudsman Act 1976* (Cth) s 5. As discussed below, 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.

for instance, a decision by an agency or officer to disclose, or not disclose, information to a third party.[58]

15.59 After completing an investigation, the Ombudsman must make a report to the agency or authority investigated, 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.[59]

15.60 The Ombudsman has no power to implement the conclusions of an investigation. However, if appropriate action is not taken, the Ombudsman can make a further report to the Prime Minister.[60] The Ombudsman must also file annual reports that are tabled in both Houses of Parliament.[61]

15.61 The Commonwealth Ombudsman has an additional role in relation to particular sectors of the Australian Government. As Law Enforcement Ombudsman, the Ombudsman must undertake an annual review of the administration of Australian

---

58 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.

59 Ibid s 15(1).

60 Ibid s 16.

61 Ibid s 19.

Federal Police conduct and practices,[62] a copy of which must be provided to both the President of the Senate and the Speaker of the House of Representatives for tabling.[63]

15.62 Another office of the Commonwealth Ombudsman is the Defence Force Ombudsman (DFO), which investigates administrative actions related to or arising out of a person's service in the Australian Defence Force (ADF), either following receipt of a complaint or on the DFO's own motion.[64] 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.[65]

Australian Public Service and Merit Protection Commissioners

15.63 The *Public Service Act* establishes the role of the APS Commissioner, whose functions include evaluating the extent to which agencies incorporate and uphold the APS Values; and the adequacy of systems and procedures in agencies for ensuring compliance with the APS Code of Conduct.[66]

15.64 Under s 44 of the Act, the APS Commissioner is required to prepare a report to the Prime Minister, for presentation to the Parliament, on the state of the APS during each financial year.[67] Every year the Commissioner sends a questionnaire to each agency seeking information to inform the report. In addition, the Commissioner reports 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.[68]

15.65 The *Public Service Act* also establishes the role of the Merit Protection Commissioner (MPC).[69] 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.[70] 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 to the minister responsible for the agency and to either or both the Prime Minister and the Presiding

---

62 *Australian Federal Police Act 1979* (Cth) pt V div 7.
63 Ibid s 40XD.
64 *Ombudsman Act 1976* (Cth) s 19C(2), (3).
65 Ibid s 19C(5)(d).
66 *Public Service Act 1999* (Cth) s 41(1)(a), (b).
67 Ibid s 44(3).
68 J Faulkner (Cabinet Secretary and Special Minister of State), *Launch of the Public Service Ethics Advisory Service: 6 May 2009* (2009) <www.smos.gov.au/speeches> at 6 December 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 Australian Federal Police: Australian Public Service Commission, *Ethics Advisory Service Client Service Charter* (2009) <www.apsc.gov.au> at 6 December 2009.
69 *Public Service Act 1999* (Cth) pt 6.
70 Ibid s 33.

Officers, for presentation to the Parliament.[71] 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.[72]

Auditor-General

15.66 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.[73] The ANAO has conducted a series of audits of the policies and practices used by Commonwealth agencies to protect their resources, including Commonwealth information.[74]

Privacy Commissioner

15.67 The Privacy Commissioner is an independent statutory office-holder established by the *Privacy Act 1988* (Cth). The Privacy Commissioner, supported by the Office of the Privacy Commissioner, is responsible for overseeing the *Privacy Act* and monitoring compliance with that Act. In the report *For Your Information: Australian Privacy Law and Practice* (ALRC 108), the ALRC made a number of recommendations directed towards clarifying and enhancing the powers of the Privacy Commissioner including, for example, introduction of a power to direct an agency to provide a Privacy Impact Assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information.[75] The Australian Government has largely supported these recommendations.[76]

Law Enforcement Integrity Commissioner

15.68 The Law Enforcement Integrity Commissioner has responsibilities in relation to the prevention, detection and investigation of serious and systemic corruption issues in

---

71 Ibid s 33(5), (6).

72 Ibid s 50.

73 Australian National Audit Office, *About Us* (2006) <www.anao.gov.au/director/aboutus.cfm> at 5 September 2008.

74 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).

75 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 47–4 and see generally Chs 45–51.

76 Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

the Australian Federal Police and the ACC.[77] The jurisdiction of the Integrity Commissioner could be invoked, for example, where unauthorised handling of Commonwealth information is associated with financial gain on the part of an officer.

15.69 In February 2009, the Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity (ACLEI) reported on its inquiry into law enforcement integrity models. The Committee considered whether ACLEI's jurisdiction should be extended beyond Commonwealth agencies with a law enforcement function, and expressed the view that, in the long term, all Commonwealth agencies with law enforcement functions should be subject to external scrutiny. The Committee suggested that further work should be done to determine a 'systematic and workable process' for extending ACLEI's jurisdiction to these other agencies.[78]

Inspector-General of Intelligence and Security

15.70 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office-holder who reviews the activities of the agencies collectively comprising the Australian Intelligence Community (AIC).[79] 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.[80]

15.71 The IGIS considers complaints or requests from ministers in relation to the actions of AIC agencies. Investigations can also be initiated on the IGIS's own motion. In undertaking inquiries, the IGIS has investigative powers similar to those of a Royal Commission. Once an inquiry is completed, the IGIS must provide a report, including any conclusions and recommendations, to the head of the relevant agency and to the responsible minister.[81] 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

---

77 *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 3.

78 Parliament of Australia—Parliamentary Joint Committee on the Australian Commission for Law Enforcement Integrity, *Inquiry into Law Enforcement Integrity Models* (2009), [5.24].

79 Agencies of the AIC are the Australian Security Intelligence Organisation; the Australian Secret Intelligence Service; the Office of National Assessments; the Defence Intelligence Organisation; the Defence Imagery and Geospatial Organisation; and the Defence Signals Directorate.

80 Inspector-General of Intelligence and Security, *About IGIS* (2008) <www.igis.gov.au/about.cfm> at 7 October 2008.

81 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 22.

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.[82]

15.72 Additional oversight of the AIC is provided by the Parliamentary Joint Committee on Intelligence and Security, which conducts an annual review of the administration, expenditure and financial statements of the AIC.[83]

Inspector-General of the ADF

15.73 The Inspector-General of the ADF (IGADF) is a statutory position introduced in 2005 to oversee the ADF military justice system.[84] 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.[85]

15.74 The IGADF does not have the power to implement measures arising out of 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.[86] The Department of Defence's annual report also includes a section on the operation of the Office of the IGADF.

Inspector-General of Taxation

15.75 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
>
> (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.

---

82 Ibid s 24.
83 The annual review is required under s 29(1)(a) of the *Intelligence Services Act 2001* (Cth).
84 *Defence Act 1903* (Cth) pt VIIIB. The position of the IGADF was introduced in the *Defence Legislation Amendment Act (No 2) 2005* (Cth).
85 Australian Government Department of Defence, *Annual Report 2006–07*, 156.
86 *Defence (Inquiry) Regulations 1985* (Cth) reg 102(3).

15.76 Where the Inspector-General, in the course of a review, forms the opinion that a tax official has engaged in misconduct, the Inspector-General must report the evidence to the Commissioner of Taxation.[87]

Information Commissioner

15.77 Although many oversight offices are potentially relevant to information-handling practices in Australian Government agencies, none of them has information handling as their primary responsibility.

15.78 As part of its anticipated reforms to FOI laws and practices, the Australian Government has proposed to establish an Office of the Information Commissioner. The proposed functions of the Information Commissioner include:

> 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).[88]

15.79 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.[89]

15.80 The proposed Information Commissioner will be supported by the Privacy Commissioner and a new FOI Commissioner.

15.81 In his report for the Department of the Prime Minister and Cabinet on information policy and e-governance in the Australian Government, Dr Ian Reinecke considered the potential roles and responsibilities of the Information Commissioner. Reinecke advised that the Information Commissioner should 'provide cross-government oversight of information policy and management and undertake a strong public advocacy role to promote open access to public sector information'.[90] The Commissioner may also have a role in reviewing, and reporting to Parliament on, agency publication schemes.[91]

---

87 *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).

88 Exposure Draft, Information Commissioner Bill 2009 (Cth) cl 9(a).

89 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009), 8.

90 I Reinecke, *Information Policy and E-governance in the Australian Government* (2009) Department of the Prime Minister and Cabinet, 34.

91 Ibid, 35.

15.82 In its Issues Paper, *Towards Government 2.0*, the Government 2.0 Taskforce noted that some aspects of Government information could fall within the purview of the proposed Information Commissioner, including information management standards, policies and guidelines, and information technology system issues. The Taskforce asked whether there were practical recommendations that it could make about how the Information Commissioner could best fulfil its functions in relation to optimising the dissemination of Government information.[92]

Submissions and consultations

15.83 Some stakeholders in this Inquiry expressed strong views about the need for independent oversight of the manner in which Australian Government agencies discharge their information-handling responsibilities. For example, Whistleblowers Australia commented on the futility of the ALRC's recommendation about information handling in the absence of formal accountability measures:

> The ALRC has made praiseworthy recommendations about information handling, awareness and understanding of secrecy obligations, and the shift towards pro-disclosure, with improved agency practices aimed at consistency, clarity and a better balance of the public interest in play.
>
> However over the last 20 years those same forms of recommendations have been made repeatedly, directions have been issued, guidelines promulgated and training courses have even been held, all to no avail. Agencies are free to administer their obligations under the FOI Act as they see fit. Similarly they may do the same in relation to whistleblowing or secrecy provisions. If one is an employee, there is simply no agency to which one can go to complain about an agency's failure to implement guidelines or legislation let alone to complain about abuses of office or other forms of maladministration. It is possible to take an agency to the [Administrative Appeals Tribunal] or the Federal Court in pursuit of some accountability but that course is totally beyond the resources of most Commonwealth employees.
>
> The bottom line is that another proposal to upgrade practices is just another round of proposals to upgrade practices. They don't actually achieve anything.[93]

15.84 Whistleblowers Australia suggested that all Commonwealth secrecy provisions, including their administration, management and enforcement, should be subject to review and investigation by ACLEI, arguing that the APSC has been ineffective in this oversight role.[94]

15.85 The Australian Press Council submitted that the process of assigning security classification levels to material should be subject to 'regular monitoring and review by an independent body'.[95] The Australia's Right to Know coalition endorsed the

---

92 Government 2.0 Taskforce, *Towards Government 2.0: An Issues Paper* (2009), Question 35. Government 2.0 and the Taskforce is explained in Ch 2.

93 Whistleblowers Australia, *Submission SR 74,* 17 August 2009.

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

95 Australian Press Council, *Submission SR 62,* 12 August 2009.

establishment of an Information Commissioner, as proposed by the Australian Government.[96]

15.86 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.[97]

15.87 In comparison, several Australian Government agencies made submissions in support of the current oversight mechanisms. The AIC submitted that there are extensive oversight mechanisms in place relating to the intelligence agencies—in particular, the IGIS.[98] The Australian Prudential Regulatory Authority advised that its mechanisms were 'as effective as is practicable'.[99] The Australian Securities and Investments Commission agreed that, in its 'limited experience', oversight mechanisms appear effective.[100]

ALRC's view

15.88 The effectiveness of the administrative reforms recommended in this report will depend on strong and independent oversight of the manner in which Australian Government agencies discharge their information-handling responsibilities.

15.89 Existing oversight mechanisms have a potential role in this context. For example, the Commonwealth Ombudsman could investigate the systemic leaking of information by Commonwealth officers in a particular agency. The APS Commissioner could report on an APS agency's administrative disciplinary system, where its operation, for example, was inadequate to promote compliance by employees with their secrecy obligations under the APS Code of Conduct. However, none of these offices has a primary role in monitoring and overseeing information-handling practices. In the ALRC's view, an Information Commissioner—such as that proposed in the Exposure Draft Information Commissioner Bill—is an important initiative to supplement current oversight of information handling by Australian Government agencies.

15.90 The ALRC recommends that the Information Commissioner's role include reviewing and reporting to the responsible minister on Australian Government agencies' information-handling policies and any directions issued to employees.[101] The ALRC considers these functions to be consistent with the functions set out in the

---

96 Australia's Right to Know, *Submission SR 72,* 17 August 2009.
97 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
98 Australian Intelligence Community, *Submission SR 37,* 6 March 2009.
99 Australian Prudential Regulation Authority, *Submission SR 12,* 13 February 2009.
100 Australian Securities & Investments Commission, *Submission SR 41,* 17 March 2009.
101 The ALRC recommends that Australian Government agencies develop and implement information-handling policies: Rec 14–1.

Exposure Draft Information Commissioner Bill and Reinecke's report on information policy and e-governance.

Recommendation 15–4 The Information Commissioner should review and report to the Minister on the information-handling policies developed by Australian Government agencies in accordance with Recommendation 14–1 and any relevant employee directions.

16. Interactions with Other Laws

Contents

Introduction

16.1 In *Freedom of Information and Privacy in Australia*, Associate Professor Moira Paterson remarked that 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.[1]

1 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [1.2].

16.2 In this chapter, the ALRC considers the relationship between Commonwealth secrecy laws and other laws dealing with the handling of Commonwealth information—namely, the *Freedom of Information Act 1982* (Cth) (FOI Act), the *Archives Act 1983* (Cth) and the *Privacy Act 1988* (Cth). The chapter also considers the interaction between secrecy laws and parliamentary privilege.

16.3 Secrecy laws may also interact with laws governing Royal Commissions and other public executive inquiries. In January 2009, the ALRC was issued with Terms of Reference for an inquiry into Royal Commissions and related issues. In the Discussion Paper, *Royal Commissions and Official Inquiries*, the ALRC proposed a model for dealing with the relationship between public executive inquiries and secrecy laws.[2] The final Report for this Inquiry was submitted to the Attorney-General on 30 October 2009. At the time of writing, the report has not yet been tabled in Parliament.

Freedom of information

16.4 The FOI Act is founded on the principle of open government. It provides a right of access to information held by government agencies and ministers. The FOI Act governs two aspects of this right. First, by requiring agencies and ministers to publish certain information,[3] and secondly, by providing persons with a right to apply for the production of documents.[4] The FOI Act also gives a person a right to access, annotate or correct records that a government agency holds about him or her.[5]

16.5 A general right of access is set out in s 11 of the FOI Act, which provides that:

> (1) Subject to this Act, every person has a legally enforceable right to obtain access in accordance with this Act to:
>
> (a) a document of an agency, other than an exempt document; or
>
> (b) an official document of a Minister, other than an exempt document.

16.6 Balanced against these access rights is the need to protect some documents from disclosure. This is expressed in the FOI Act by the exemption provisions. 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.[6]

---

2 Australian Law Reform Commission, *Royal Commissions and Official Inquiries*, Discussion Paper 75 (2009), Proposal 17–2.

3 *Freedom of Information Act 1982* (Cth) pt II.

4 Ibid pt III.

5 Ibid pt V.

6 Ibid s 3(1)(b).

16.7 Notwithstanding that a document may fall within an exemption category, an agency or minister may nevertheless be required to provide an applicant with access to an edited copy from which any exempt matter has been deleted.[7] 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.

16.8 The following discussion focuses on the interaction between the FOI Act and secrecy provisions. First, this section sets out a general overview of the exemption provisions under the FOI Act, including proposed government reforms. This chapter then discusses the specific secrecy exemption set out in s 38 of the FOI Act, as well as the interaction between FOI and those secrecy provisions outside the s 38 exemption, and assesses the need for an override provision. Finally, the ALRC makes recommendations for reform.

Exemptions under the FOI Act

16.9 As noted above, the FOI Act provides members of the public with a general right of access to government documents, limited by specific exemptions. Exemptions fall within three broad categories: agency-based exemptions; class-based exemptions; and harm-based exemptions.

Agency-based exemptions

16.10 Section 7 of the FOI Act operates to exempt certain agencies from the Act altogether. Most of these agencies have functions relating to national security, including the Inspector-General of Intelligence and Security (IGIS) and the six agencies comprising the Australian Intelligence Community (AIC).[8] Section 7(2A) also provides an exemption for all agencies in relation to documents that originate with, or have been received from, the AIC or the IGIS. A number of other agencies are exempt from the operation of the FOI Act in relation to particular documents—often those relating to an agency's commercial functions.[9]

---

7 Ibid s 22.

8 Ibid s 7(1), (1A). The AIC agencies are: the Australian Secret Intelligence Service, the Australian Security Intelligence Organisation, the Office of National Assessments, the Defence Imagery and Geospatial Organisation; the Defence Signals Directorate; and the Defence Intelligence Organisation. Other exempt agencies include, eg, the Auditor-General, Australian Government Solicitor (AGS) and the National Workplace Relations Consultative Council.

9 Ibid s 7(2). These include, eg, the Australian Broadcasting Corporation and the Special Broadcasting Service, in relation to their program material and datacasting content; and the Commonwealth Scientific and Industrial Research Organisation, in relation to documents in respect of its commercial activities.

Class-based exemptions

16.11 Class-based exemptions apply to documents of a certain nature, such as Cabinet documents.[10] Other class-based exemptions are for Executive Council documents;[11] where secrecy provisions[12] or legal professional privilege apply;[13] where disclosure would be in contempt of parliament or contempt of court;[14] electoral rolls;[15] and certain documents arising under companies and securities legislation.[16]

16.12 A class-based exemption will be satisfied wherever a document falls within a particular category. There is no additional assessment of the merits of disclosure, or the potential harm that disclosure may cause. To the extent that there is a notion of public interest, it is implicit—in that the Parliament has decided that the release of any of the documents in one of the specified categories under the FOI Act would not be in the public interest.

Harm-based exemptions

16.13 This category of exemptions depends on demonstrating the harm that would or could reasonably be expected to be caused by disclosure. For example, documents 'affecting national security, defence or international relations' are exempt under 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.

16.14 Other exemptions in this category include harms to: Commonwealth-State relations;[17] law enforcement and public safety;[18] the financial or property interests of the Commonwealth;[19] operations of agencies;[20] business and professional affairs;[21] research;[22] the national economy;[23] and material obtained in confidence.[24]

---

10 If it meets the definition of Cabinet document in s 34(1).
11 *Freedom of Information Act 1982* (Cth) s 35.
12 Ibid s 38. The exemption for documents containing information that is the subject of certain secrecy provisions is considered in detail below.
13 Ibid s 42.
14 Ibid s 46.
15 Ibid s 47A.
16 Ibid s 47.
17 Ibid s 33A.
18 Ibid s 37.
19 Ibid s 39.

Proposed Government reforms

16.15 The FOI Act is currently the subject of proposed reforms[25] set out in the Exposure Draft of the Freedom of Information Amendment (Reform) Bill 2009 (FOI Exposure Draft Bill).

16.16 The FOI Exposure Draft Bill proposes to repeal a number of class-based exemptions, including for Executive Council documents; documents arising out of companies and securities legislation; and documents relating to the conduct by an agency of industrial relations.[26] The proposed amendments would also narrow the Cabinet exemption to documents 'at the core of the Cabinet process'.[27]

16.17 Further, the Exposure Draft proposes to amend many existing exemptions to make them subject to a public interest test. As explained by the then Cabinet Secretary and Special Minister of State, Senator the Hon John Faulkner:

> 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'.[28]

16.18 Exemptions concerning personal privacy,[29] business affairs,[30] the national economy[31] and research[32] would all become conditional exemptions.[33]

The secrecy exemption

16.19 Section 38 of the FOI Act contains an exemption from the requirement to disclose for those documents that are, or information contained in documents that is, subject to certain secrecy provisions (the secrecy exemption).

---

20 Ibid s 40.
21 Ibid s 43.
22 Ibid s 43A.
23 Ibid s 44.
24 Ibid s 45.
25 Many of these reforms were 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).
26 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 2.
27 J Faulkner (Cabinet Secretary and Special Minister of State), *Freedom of Information (FOI) Reform: Companion Guide* (2009). See Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) cl 34.
28 J Faulkner (Cabinet Secretary and Special Minister of State), *Open and Transparent Government—the Way Forward* (2009) <www.smos.gov.au/speeches/2009/sp_20090324.html> at 26 November 2009.
29 *Freedom of Information Act 1982* (Cth) s 41.
30 Ibid s 43.
31 Ibid s 44.
32 Ibid s 43A.
33 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 2 pt 2 div 3.

16.20 The secrecy exemption, as it was originally enacted in 1982, applied to any document if there was 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.[34]

16.21 In 1991, however, the exemption was significantly narrowed to apply where:

> (a) disclosure of the document, or information contained in the document, is prohibited under a provision of an enactment; and
>
> (b) either:
>
> (i) that provision is specified in Schedule 3; or
>
> (ii) this section is expressly applied to the document, or information, by that provision, or by another provision of that or any other enactment.[35]

16.22 Section 38(1A) makes it clear that an individual's right to access information applies in circumstances in which the secrecy provision does not prohibit disclosure—for example, where disclosure is permitted under an exception to the secrecy provision.

16.23 The *FOI Guidelines—Exemption Sections in the FOI Act* (FOI Exemption Guidelines), prepared by the Australian Government Solicitor, express the policy position 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.[36]

Which secrecy provisions are covered?

16.24 Currently, sch 3 specifies more than 65 secrecy provisions from over 28 Acts and one sub-regulation as subject to the secrecy exemption in s 38. In addition, the ALRC has identified four provisions that expressly apply s 38 but which are not listed in sch 3.[37]

---

34 *Freedom of Information Act 1982* (Cth) s 38(1) (as originally enacted).

35 Ibid s 38(1).

36 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [9.1.4]. See also Australian Government Attorney-General's Department, *Freedom of Information Act 1982—Fundamental Principles and Procedures* (2005) <www.pmc.gov.au/> at 26 November 2009.

37 *National Health Security Act 2007* (Cth) s 90; *Australian Prudential Regulation Authority Act 1998* (Cth) s 56; *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C; *Reserve Bank Act 1959* (Cth) s 79A.

16.25 Provisions listed in the secrecy exemption include:

- health and welfare secrecy provisions, directed towards the protection of personal information;[38]
- secrecy provisions that protect various types of information obtained by regulatory agencies;[39]
- national security and defence secrecy provisions;[40] and
- taxation and superannuation secrecy provisions.[41]

Scope of the secrecy exemption

16.26 There are limits to the application of the secrecy exemption. As explained by Paterson, a document is exempt under the secrecy exemption 'only to the extent that a complying secrecy provision prohibits its disclosure'.[42] For example, in *Duncan and Department of Health and Ageing*, the Administrative Appeals Tribunal (AAT) held that parts of information protected under the *Aged Care Act 1997* (Cth) could be released to the applicant on the basis of the exception in s 86-3, which permitted the Secretary of the Department to disclose information if he or she certified, in writing, that such disclosure was necessary in the public interest.[43]

16.27 In addition, the secrecy exemption does not apply if the relevant document or information contains personal information that relates only to the person making the request,[44] and s 503A of the *Migration Act 1958* (Cth) does not apply.[45]

Overlap with other FOI exemptions

16.28 Much of the information protected through the secrecy exemption may also fall within other FOI exemptions—in particular, exemptions relating to business affairs, personal privacy and the operations of agencies.

---

38 For example, *Aged Care Act 1997* (Cth) ss 86-2, 86-5, 86-6, 86-7; *Child Support (Assessment) Act 1989* (Cth) s 150; *Australian Institute of Health and Welfare Act 1987* (Cth) s 29.

39 For example, *Designs Act 2003* (Cth) ss 61, 108; *Civil Aviation Act 1988* (Cth) s 32AP.

40 For example, *Intelligence Services Act 2001* (Cth) s 41; *Defence (Inquiry) Regulations 1985* (Cth) reg 63; *Australian Security Intelligence Organisation Act 1979* (Cth) s 92.

41 For example, *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C; *Fringe Benefits Tax Assessment Act 1986* (Cth) s 5; *Income Tax Assessment Act 1936* (Cth) s 16.

42 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.97].

43 *Duncan and Department of Health and Ageing* [2004] AATA 747.

44 *Re Richardson and Federal Commissioner of Taxation* (2004) 81 ALD 486, 503; *Petroulias v Commissioner of Taxation* [2006] AATA 333, [65]–[66].

45 *Freedom of Information Act 1982* (Cth) s 38(2), (3). The *Migration Act 1958* (Cth) s 503A is discussed below.

16.29 For example, one of the secrecy provisions listed in the exemption is s 187 of the *Gene Technology Act 2000* (Cth), which protects 'confidential commercial information' obtained by officers in the course of performing functions or duties under gene technology regulatory laws. In comparison, s 43 of the FOI Act provides an exemption for documents relating to business affairs, defined to include:

> (a) trade secrets;
>
> (b) 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
>
> (c) information (other than trade secrets or information to which paragraph (b) applies) concerning a person in respect of his or her business or professional affairs or concerning the business, commercial or financial affairs of an organization or undertaking, being information:
>
> (i) 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 organization or undertaking in respect of its lawful business, commercial or financial affairs; or
>
> (ii) the disclosure of which under this Act 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.

16.30 'Confidential commercial information' communicated under the *Gene Technology Act* would almost always fall within one of the above categories. Typically, the information would have some commercial value, which would be diminished by disclosure. Even where there was no such commercial value, release of the information might 'unreasonably affect' the organisation in undertaking its business, commercial or financial affairs.

16.31 Similarly, many of the provisions listed in the secrecy exemption apply to sensitive categories of personal information, including health,[46] taxation[47] and welfare[48] information. In comparison, under s 41 of the FOI Act, an exemption applies if disclosure of a document 'would involve the unreasonable disclosure of personal information about any person (including a deceased person)'.

16.32 Finally, s 40(1)(d) of the FOI Act provides an exemption for documents which may 'have a substantial adverse effect on the proper and efficient conduct of the operations of an agency'. This exemption has successfully been used, for example, by

---

46 For example, *Aged Care Act 1997* (Cth) ss 86-5, 86-6; *Australian Institute of Health and Welfare Act 1987* (Cth) s 29; *Disability Services Act 1986* (Cth) s 28; *National Health Act 1953* (Cth) s 135A.

47 For example, *Taxation Administration Act 1953* (Cth) ss 3C, 3G, 8XB, 8WB, sch 1 s 355-5; *Income Tax Assessment Act 1936* (Cth) s 16.

48 For example, *Child Support (Assessment) Act 1989* (Cth) s 150; *Child Support (Registration and Collection) Act 1988* (Cth) s 16.

the Australian Competition and Consumer Commission (ACCC) to protect from disclosure certain documents provided to it by telecommunications companies. The Deputy President of the AAT upheld the use of the exemption on the basis of the ACCC's need to obtain industry information voluntarily in the future.[49]

16.33 The ALRC has identified two provisions listed in the secrecy exemption in the area of national security.[50] Section 41 of the *Intelligence Services Act 2001* (Cth) and s 92 of the *Australian Security Intelligence Organisation Act 1979* (Cth) prohibit any person from disclosing information that identifies, or could reasonably lead to the identification of, a person who is or has been an agent or staff member of the Australian Secret Intelligence Service (ASIS) or the Australian Security Intelligence Organisation (ASIO), respectively.

16.34 As noted above, pursuant to s 7 of the FOI Act, the AIC agencies are completely exempt from the operation of the Act. In addition, any other agency is exempt from the operation of the Act in relation to a document that originated with, or was received from, an AIC agency.[51] Further, s 33(1)(a) of the FOI Act provides an exemption for documents that 'would or could reasonably be expected to, cause damage to the security of the Commonwealth'. An equivalent exemption in the *Archives Act* has been interpreted to include documents that reveal, or would assist in revealing, the identity of an ASIO informant.[52]

Inter-jurisdictional comparisons

16.35 FOI legislation in many other jurisdictions includes exemptions based on secrecy provisions. One of the broadest is s 44 of the *Freedom of Information Act 2000* (UK), which provides that information is exempt if its disclosure is 'prohibited by or under any enactment'. Pursuant to this exemption, there are 'hundreds of statutory provisions that prevent the release of information'.[53] Similarly, in New Zealand, a request for the release of official information under the *Official Information Act 1982* (NZ) may be refused where making the information available would 'be contrary to the provisions of a specified enactment'.[54]

16.36 Section 24 of the *Access to Information Act 1985* (Canada) includes a similar secrecy exemption to s 38 of the FOI Act, which applies to those secrecy provisions set out in a schedule to the Act. The Canadian exemption goes further than its Australian

---

49 *Re Telstra Australia Limited and Australian Competition and Consumer Commission* [2000] AATA 71.

50 *Intelligence Services Act 2001* (Cth) s 41; *Australian Security Intelligence Organisation Act 1979* (Cth) s 92.

51 *Freedom of Information Act 1982* (Cth) s 7(2A).

52 *Re Throssell and Australian Archives* (1987) 14 ALD 292.

53 Information Commissioner's Office (UK), *Freedom of Information Act Awareness Guidance No 27: Prohibitions on Disclosure* (January 2006), 2.

54 *Official Information Act 1982* (New Zealand) s 18(c)(i).

counterpart, however, by *requiring* the nondisclosure of such information.[55] It also establishes a committee to review the provisions in the schedule and to report 'on whether and to what extent the provisions are necessary'.[56] The Canadian Office of the Information Commissioner has strongly criticised s 24. In its *Response to the Report on Access to Information Review Task Force*, the Office admonished the 'whittling away of the right of access' under the section and recommended that the section be abolished.[57]

16.37 Secrecy provisions also form a common basis for exemption from FOI legislation at the Australian state and territory level. Older secrecy exemptions, such as those in the FOI legislation in Victoria and the ACT, mirror the broad wording of the original federal secrecy exemption.[58] In comparison, more recently enacted secrecy exemptions follow the approach of the current federal FOI Act, by only applying the exemption to a specific list of secrecy offences. Most notably, this approach has been followed in the *Right to Information Act 2009* (Qld) and the *Government Information (Public Access) Act 2009* (NSW).

16.38 The *Right to Information Act 2009* (Qld), which commenced on 1 July 2009, gives legislative effect to most of the recommendations of the independent review of the state's FOI legislation chaired by Dr David Solomon (the Solomon Review).[59] One of the few areas in which the Act diverges from the Solomon Review's recommendations is with respect to the secrecy exemption. The review recommended that the secrecy exemption—set out in sch 1 of the former Queensland FOI legislation—should be removed and, instead, the existence of a secrecy provision should be a relevant factor in assessing whether disclosure is warranted under a general public interest test.[60] The Queensland Government did not accept this recommendation:

> Schedule 1 provides a very limited list of secrecy provisions in other legislation relating to the protection of the rights or safety of citizens. These matters require an absolute guarantee of confidentiality to ensure upfront public confidence and participation in certain processes of government. For example, Schedule 1 protects the confidentiality of the witness protection program, adoption information, child protection notifications and personal taxation information. The government considers there is a compelling public interest in protecting this information from public disclosure in all circumstances. In addition, the exemption for audit information … is considered necessary to protect the confidentiality of information obtained during the

55 As noted above, exempt documents under the *Freedom of Information Act 1982* (Cth) are not subject to the Act's general disclosure requirement, however, an Australian Government agency or minister may choose to release them.

56 *Access to Information Act 1985* (Canada) s 24(2).

57 Office of the Information Commissioner (Canada), *Annual Report* (1999–2000), Appendix A, pt A.

58 *Freedom of Information Act 1982* (Vic) s 38; *Freedom of Information Act 1989* (ACT) s 38. The federal secrecy provision exemption, as originally enacted, is set out above.

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

60 Ibid, 156–157, Rec 45.

> course of audits and to maintain the integrity of the Queensland Audit Office's audit process, which is comparable to exemptions provided in other jurisdictions.[61]

16.39 A similar approach is also being adopted by the *Government Information (Public Access) Act 2009* (NSW), which received assent on 26 June 2009.[62] Instead of retaining an automatic exemption for documents covered by a secrecy provision—as is the case under the former *Freedom of Information Act 1989* (NSW)—the Act lists approximately 20 secrecy provisions, which conclusively establish an 'overriding public interest against disclosure'.[63] The fact that information is subject to any other secrecy provision will be a relevant consideration in applying the public interest test on a case-by-case basis.[64]

16.40 In contrast, however, the secrecy exemption in the Tasmanian FOI Act ceased to have effect three years after commencement of the Act.[65] There is no exemption from disclosure for information protected by secrecy provisions in the *Right to Information Bill 2009* (Tas).

Previous inquiries and the secrecy exemption

16.41 The secrecy exemption in the FOI Act has been considered in a number of previous inquiries. In the 1995 report, *Open Government: A Review of the Federal Freedom of Information Act* (ALRC 77), the ALRC and Administrative Review Council (ARC) recommended that the secrecy exemption should be repealed on the basis that the other FOI exemptions—such as those dealing with personal information, national security and defence—provided sufficient protection for the information covered by secrecy provisions.[66] The Report noted the submission by the then Department of Social Security that removal of the secrecy exemption for FOI applications to the Department had not adversely affected the Department's operations.[67]

16.42 The ALRC and ARC 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.[68]

16.43 In 2001, several recommendations made in ALRC 77 were considered as part of the Senate Legal and Constitutional Affairs Committee *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (the Senate Committee

---

61 Queensland Government, *The Right to Information: A Response to the Review of Queensland's Freedom of Information Act* (2008).
62 At the time of writing, the commencement date had not been proclaimed.
63 *Government Information (Public Access) Act 2009* (NSW) sch 1.
64 Ibid s 14.
65 *Freedom of Information Act 1991* (Tas) s 36.
66 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), Rec 70.
67 Ibid, [11.3].
68 Ibid.

Inquiry).[69] In its submission to the Senate Committee Inquiry, the Australian Government Attorney-General's Department (AGD) opposed the repeal of the secrecy exemption:

> 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.[70]

16.44 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'.[71]

16.45 The FOI Exposure Draft Bill and Companion Guide do not expressly address the secrecy exemption.

Interaction between the FOI Act and other secrecy provisions

16.46 The relationship between secrecy laws and the FOI Act goes beyond the specific secrecy exemption. A particular issue that arises is whether there is a need for a provision in the FOI Act to expressly override secrecy provisions.

16.47 In accordance with the general right of access set out in s 11 of the FOI Act, in the absence of the secrecy exemption or another applicable FOI exemption, access will be available to a document to which a secrecy provision applies.

16.48 However, some ambiguity in the relationship between other secrecy provisions and the FOI Act has arisen as a result of the finding of the Federal Court in *Kwok v Minister for Immigration and Multicultural Affairs* (*Kwok*).[72] In this case, Tamberlin J considered whether the secrecy exemption applied to information protected by the secrecy provision in s 503A of the *Migration Act* (restricting the disclosure by Commonwealth officers of information supplied by law enforcement agencies or intelligence agencies). Notwithstanding that the provision was not listed in sch 3 of the FOI Act, nor expressly applied the secrecy exemption, Tamberlin J considered that the 'comprehensive language' of the *Migration Act* provision was sufficient to exclude the operation of the FOI Act.[73]

---

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

70 Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (2001), [3.35].

71 Ibid, [3.34]–[3.36].

72 *Kwok v Minister for Immigration and Multicultural Affairs* (2001) 112 FCR 94.

73 Ibid, 99.

16.49 The decision in *Kwok* has been subject to criticism.[74] Although the decision was overturned by a Full Court of the 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.[75] While this amendment dealt with the immediate problem created by *Kwok*, it remains uncertain whether information subject to a secrecy provision may be exempt although the secrecy provision does not meet the criteria set out in s 38.

16.50 The FOI Acts in some other jurisdictions make the relationship between FOI and secrecy provisions clear by explicitly overriding prohibitions on nondisclosure in other legislation. For example, s 11 of the *Government Information (Public Access) Act 2009* (NSW) provides that:

> This Act overrides a provision of any other Act or statutory rule that prohibits the disclosure of information (whether or not the prohibition is subject to specified qualifications or exceptions), other than a provision of a law listed in Schedule 1 as an overriding secrecy law.

16.51 An equivalent provision in the *Right to Information Act 2009* (Qld) makes clear that '[t]his Act overrides the provisions of other Acts prohibiting the disclosure of information (however described)'.[76]

Impact on individual officers

16.52 What is the situation where an officer discloses information in accordance with the FOI Act but this action is potentially in breach of a secrecy provision?

16.53 Many secrecy provisions permit disclosure in the course of a Commonwealth officer's duties. This has been interpreted as encompassing FOI and other routine disclosures.[77] There is the potential for conflict, however, where a secrecy provision does not have any such exception, or where the exception is more narrowly framed—including, for example, permitting disclosures in the 'performance of duties under this Act'. In the secrecy provision at issue in *Kwok*,[78] discussed above, the only permissible disclosures of the information were to a minister or an 'authorised migration officer' for the purpose of allowing them to exercise certain statutory powers.[79]

---

74 See, eg, M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.99].

75 *Migration Legislation Amendment (Protected Information) Act 2003* (Cth) sch 2.

76 *Right to Information Act 2009* (Qld) s 6.

77 Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [9.1.4], citing *Canadian Pacific Tobacco Co Ltd v Stapleton* (1952) 86 CLR 1. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.98].

78 *Kwok v Minister for Immigration and Multicultural Affairs* (2001) 112 FCR 94.

79 *Migration Act 1958* (Cth) s 503A.

16.54 Some protection for individual officers is provided by s 92(1)(b) of the FOI Act. Pursuant to this section, an authorised officer[80] who gives access to a document in 'the bona fide belief that access was required' by the FOI Act cannot be liable for criminal prosecution under a secrecy offence.[81] An equivalent provision in s 91(1) protects an officer who discloses information in these circumstances from any civil action in defamation, breach of confidence or infringement of copyright.

16.55 In ALRC 77, the ALRC and ARC criticised the lack of protection that s 91 provided to officers who release non-exempt documents outside of a formal FOI Act application process, and 'non-sensitive exempt information'.[82] The ALRC and ARC recommended that s 91 should be extended to apply to the release of a non-exempt document other than under the FOI Act and to an exempt document under or outside the FOI Act pursuant to a bona fide exercise of discretion not to claim the exemption.[83] This is similar to the approach taken in the FOI Exposure Draft Bill, which would amend ss 91 and 92 to provide protection to an officer who:

> (a) publishes a document in good faith, in the belief that the publication is required or permitted under Part II (information publication scheme) or section 11C (publication of information in accessed documents); or
>
> (b) gives access to a document in good faith, in the belief that the access is required or permitted to be given in response to a request; or
>
> (c) publishes, or gives access to, a document in good faith, in the belief that the publication or access is required or permitted otherwise than under this Act (whether or not under an express legislative power).[84]

16.56 The Australian Public Service (APS) Commissioner's Annual Report 2007–08 highlighted several cases that had come before the Merit Protection Commissioner (MPC) during the reporting period. One of these involved an APS employee who had been subject to administrative sanctions for mistakenly releasing a document under the FOI Act which contained confidential personal information. In part, the finding of misconduct was based on the duty of non-disclosure in reg 2.1 of the *Public Service Regulations 1999* (Cth). The MPC found that 'the practical intent of this regulation was not to cover the situation where an FOI officer makes a mistake and releases information that should have been withheld' and therefore recommended that the finding of misconduct be set aside on this issue.[85]

---

80 That is, an officer to whom the responsible Minister or principal officer of the agency has given authority to make decisions about FOI access: *Freedom of Information Act 1982* (Cth) s 23.

81 See also *Actors' Equity v Australian Broadcasting Tribunal* (1984) 6 ALD 68, 80–81.

82 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [4.20]–[4.21].

83 Ibid, Recs 10, 11. The ALRC and ARC did not address whether there was a need for equivalent recommendations in the context of s 92, which protects against criminal prosecution.

84 Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 4 pt 1 cll 50, 57.

85 Australian Public Service Commissioner, *Annual Report 2007–08* (2008), 'Review of actions case studies'.

Submissions on Issues Paper

16.57 In the Issues Paper, *Review of Secrecy Laws* (IP 34), the ALRC asked several questions about the relationship between the FOI Act and secrecy provisions.[86] In particular, the ALRC sought views on whether the secrecy exemption should be repealed or amended.[87]

16.58 Some government agencies strongly supported retaining the secrecy exemption.[88] For example, the Australian Taxation Office (ATO) raised concerns that repealing the exemption could generate uncertainty for taxpayers and tax officers about the applicable level of protection.[89] The Australian Prudential Regulation Authority (APRA) commented that:

> 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 information.[90]

16.59 Other stakeholders supported the repeal of the secrecy exemption, generally noting that the other exemption categories were sufficient to provide protection even where secrecy provisions existed. For example, the Australia's Right to Know (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).[91]

16.60 Some stakeholders submitted that if a secrecy exemption like s 38 were retained, it should be subject to a public interest test.[92] For example, the Public Interest Advocacy Centre (PIAC) suggested that, in some contexts there should be a prima facie exemption—such as for documents prepared by or received from a security agency—but 'the exemption itself should be tested having regard to the content of the

---

86 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Questions 7–1 to 7–3.

87 Ibid, Question 7–2(b).

88 See, eg, 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 Australian Taxation Office, *Submission SR 13,* 16 February 2009.

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

91 Australia's Right to Know, *Submission SR 35,* 6 March 2009.

92 See, eg, Media Entertainment & Arts Alliance, *Submission SR 39,* 10 March 2009.

document itself, the possible consequences of release, and any positive public interest factors in favour of disclosure'. In PIAC's view, disclosure in accordance with the FOI Act should override secrecy provisions in other Acts. PIAC also identified a 'lack of coherence in the range and seriousness of matters excluded from FOI law by the operation of section 38'.[93]

16.61 Ron Fraser suggested that while other exemption provisions in the FOI Act may not 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. ... 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.[94]

16.62 In Fraser's view, the only secrecy provisions that should be included in a secrecy exemption are 'those that protect information, access to which cannot be determined under other FOI exemptions'.[95] Accordingly, he 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.[96]

16.63 Fraser further suggested the repeal of s 38(1)(b)(ii)—which extends the exemption to secrecy provisions that 'expressly apply' s 38. In his view, this would ensure maximum transparency of the secrecy provision's application.[97]

16.64 The AGD raised concerns about a potential conflict between the requirement to disclose under the FOI Act and secrecy provisions that do not contain an exception for disclosures required by or authorised by law and are not listed in the secrecy exemption. For these documents, the AGD submitted that 'it might be helpful to clarify that a disclosure … authorised under the FOI Act does not constitute an offence under secrecy laws.[98]

---

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

94 R Fraser, *Submission SR 42,* 23 March 2009.

95 Ibid. So, eg, he suggested that the exemptions concerning personal information and business affairs, which already include a number of safeguards for 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"'.

96 Ibid.

97 Ibid.

98 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.

Discussion Paper proposals

16.65 In the Discussion Paper, *Review of Secrecy Laws* (DP 74), the ALRC noted the ongoing concern expressed by some agencies that the removal of the secrecy exemption would undermine the confidence of individuals and others providing information to government. However, the ALRC expressed the preliminary view that the FOI exemptions provide sufficient protection for information that is the subject of secrecy provisions, without the need for the additional protection provided by the secrecy exemption. The ALRC proposed that the existence of a secrecy provision should constitute a relevant factor when a decision maker considers whether disclosure under another exemption provision would be contrary to the public interest.[99]

16.66 On the above policy rationale, the ALRC proposed that the secrecy exemption should be repealed.[100] The ALRC made two further consequential proposals directed towards clarifying the relationship between secrecy provisions and the FOI Act:

- the Office of Parliamentary Counsel should issue a drafting direction requiring secrecy provisions to indicate expressly whether they override the FOI Act;[101] and

- the FOI Exemption Guidelines should provide guidance to FOI officers on the need to consider relevant secrecy provisions when evaluating whether information should be disclosed under exemption provisions.[102]

16.67 The ALRC recognised, however, that its proposal to repeal the secrecy exemption was likely to be contentious. It therefore considered other possible reforms, should the provision be retained. The ALRC emphasised the need for clarity in the manner in which the provision operated—in particular, the need for any new secrecy provision to address explicitly its interaction with the FOI Act. The ALRC further proposed that sch 3 should be reviewed in accordance with the pro-disclosure policy expressed in the objects of the FOI Exposure Draft Bill, and updated regularly.[103]

Submissions on Discussion Paper

Repeal of the secrecy exemption

16.68 A number of Australian Government agencies expressed the view that the proposed repeal of the secrecy exemption would adversely affect their functions,[104]

---

99 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 4–3.

100 Ibid, Proposal 4–1.

101 Ibid, Proposal 4–2.

102 Ibid, Proposal 4–3.

103 Ibid, Proposal 4–4.

104 See, eg, IP Australia, *Submission SR 76,* 19 August 2009; The Treasury, *Submission SR 60,* 10 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; Australian Prudential Regulation Authority, *Submission SR 52,* 6 August 2009. The Australian Intelligence Community did not support the

several reiterating concerns raised in response to IP 34. For example, APRA commented that the repeal would lead to uncertainty about whether non-publicly available information provided by regulated entities could be released under FOI. This would 'fundamentally alter how regulated entities approach their dealings with APRA', including the potential for less candid communication.[105]

16.69 The ATO also expressed strong concerns about the potential uncertainty that could result from repeal of the secrecy exemption. In the ATO's view, the possibility that information might be released under FOI could prejudice the conduct of investigations or the willingness of foreign governments to provide information to the ATO. It suggested that:

> a distinction [should] be drawn between information relating to the workings of government departments and information which is collected by regulatory agencies, such as the ATO, Centrelink and [the Australian Securities and Investments Commission] which is inherently confidential in that it relates to individuals and businesses and not to the workings of government.[106]

16.70 The ATO also commented that—because of the exception in tax secrecy laws for disclosures in accordance with an officer's duties—repeal of s 38 could lead to 'the anomalous outcome' of a tax officer being compelled to disclose information under the FOI Act where that disclosure would not otherwise be permitted under the tax secrecy provision.[107]

16.71 Similar issues were raised by the Treasury, including that the public interest test under some FOI exemptions meant that the repeal of the secrecy exemption 'would in effect render some types of secret material more secret than others'.[108] The Treasury proposed that a more effective way of addressing concerns about the breadth of secrecy provisions included in the FOI exemption might be

> through ensuring that the initial judgment of when material is 'secret' is appropriately limited by ensuring, for instance, as is the case with secrecy provisions relating to agencies such as APRA and the ATO, that these provisions are designed to give effect to the public expectation that the confidentiality of information provided to Government is respected.[109]

16.72 IP Australia noted that repeal of the secrecy exemption could raise challenges for Australia's patents and designs system, including the potential for the release of

---

proposal to the extent that it will decrease the protections afforded by s 41 of the *Intelligence Services Act 2001* (Cth) and s 92 of the *Australian Security Intelligence Organisation Act 1979* (Cth): Australian Intelligence Community, *Submission SR 77,* 20 August 2009.

105 Australian Prudential Regulation Authority, *Submission SR 52,* 6 August 2009. See also IP Australia, which raised concerns about business competitors seeking access to documents: IP Australia, *Submission SR 76,* 19 August 2009.

106 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

107 Ibid.

108 The Treasury, *Submission SR 60,* 10 August 2009.

109 Ibid.

information outside the open access period to infringe Australia's international obligations under art 21 of the *Patent Cooperation Treaty*.[110] It further suggested that removal of the section could also create conflict between provisions of the FOI Act and prohibitions on disclosure in patents and designs legislation.[111]

16.73 On the other hand, civil liberties groups and media organisations supported the proposed repeal of the secrecy exemption, agreeing that it would 'promote a culture of openness'[112] and that the other exemption provisions in the FOI Act provided sufficient protection for government information.[113] The ARTK coalition also commented that:

> public officials would still retain the protection of s 92(1) whereby an officer authorises access to a document in the bona fide belief that access was required by the FOI Act, then the authorising officer, and any other person involved in granting access, is protected from criminal prosecution under any applicable secrecy law.[114]

16.74 Indigenous Business Australia (IBA)—whose secrecy provisions are not currently listed in sch 3 of the FOI Act—also expressed support for the proposed repeal of the secrecy exemption.[115] Further, IBA noted that the decision in *Kwok* has created uncertainty about the provision's application, which could result in the inconsistent application of legal obligations.[116] IBA also noted that:

> In practice, many documents subject to s 191 [of the *Aboriginal and Torres Strait Islander Act 2005* (Cth)] are exempt from disclosure on the basis of specific grounds of exemption under Part IV of the FOI Act, particularly those that concern personal privacy and business affairs. In addition, documents pertaining to IBA's commercial activities are also exempt from disclosure pursuant to s 11 and Sch 2, Part II, Div 1 of the FOI Act.[117]

16.75 The Department of Health and Ageing (DoHA) agreed with the ALRC's view that the other exemptions in the FOI Act, such as the privacy exemption, would adequately cover secrecy provisions 'in many circumstances'. However, DoHA

---

110 *World Intellectual Property Organisation: Patent Cooperation Treaty*, 19 June 1970, (entered into force generally on 1 April 2002).

111 IP Australia, *Submission SR 76,* 19 August 2009. Compare submission from Ron Fraser, that s 40(1)(d) of the FOI Act (substantial adverse effect on conduct of operations of an agency) would provide an appropriate exemption in cases that do not fall within other exemptions, such as s 61 of the *Designs Act 2003* (Cth) and s 56 of the *Patents Act 1990* (Cth): R Fraser, *Submission SR 78,* 21 August 2009.

112 Civil Liberties Australia, *Submission SR 47,* 27 July 2009. See also Liberty Victoria, *Submission SR 50,* 5 August 2009.

113 Australia's Right to Know, *Submission SR 72,* 17 August 2009. See also R Fraser, *Submission SR 78,* 21 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009. The Non-Custodial Parents Party submitted that FOI provisions should always prevail over secrecy provisions: Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009.

114 Australia's Right to Know, *Submission SR 72,* 17 August 2009.

115 Indigenous Business Australia, *Submission SR 64,* 13 August 2009. The Department of Human Services agreed that it was desirable that the relationship between secrecy provisions and the FOI Act be clarified but did not express a view on the appropriate solution: Department of Human Services, *Submission SR 83,* 8 September 2009.

116 The ARTK coalition also raised this issue: Australia's Right to Know, *Submission SR 72,* 17 August 2009.

117 Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

suggested that there were particular features of the information collected under the *Aged Care Act* that make it preferable to protect it through specific secrecy provisions rather than the FOI Act's privacy exemption—in particular, the difficulty of consulting with the individuals to whom the information relates (as required under s 41 of the FOI Act).[118] The Social Security Appeals Tribunal (SSAT) commented that, should the secrecy exemption be repealed, it would require some other protection for its adjudicative functions.[119]

16.76 The Department of Immigration and Citizenship advised of a potential conflict of laws should the secrecy exemption be repealed. Section 503A of the *Migration Act* prohibits an officer from examining documents, other than for the review of visa decisions and, if the secrecy exemption were repealed,

> it would cause an unacceptable legal conflict in which an FOI officer would on the one hand be required to consider a section 503A document for disclosure and on the other hand be forbidden from examining the document for the purposes of an FOI request. This conflict would need to be addressed in any legislation change proposed.[120]

Drafting directions

16.77 Several stakeholders supported the issuing of drafting directions, which would require secrecy provisions to indicate expressly whether they override the FOI Act.[121] Fraser, however, argued that such a direction could be counterproductive and 'serve as an invitation to some agencies to seek to avoid the FOI Act'. He suggested that, in the alternative, a government policy should be adopted that a secrecy provision can only override the FOI Act in 'exceptional circumstances', such as:

> where information protected by a secrecy provision could not be subject to claims under existing FOI exemptions, and the disclosure of such information would cause substantial adverse harm to a significant public interest.[122]

16.78 Fraser further noted that:

> The proposed Drafting Direction does not directly address the situation where a later secrecy provision could be held to be inconsistent with the general provisions for disclosure in the FOI Act. … It might be advisable for the FOI Act itself additionally to provide that later legislative provisions do not override the FOI Act unless they specifically provide for that, and, if appropriate, to include a note as to the Drafting Direction.[123]

---

118 Department of Health and Ageing, *Submission SR 81,* 28 August 2009.
119 Social Security Appeals Tribunal, *Submission SR 79,* 24 August 2009.
120 Department of Immigration and Citizenship, *Submission SR 59,* 7 August 2009.
121 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.
122 R Fraser, *Submission SR 78,* 21 August 2009.
123 Ibid.

Secrecy provisions as a relevant factor in balancing the public interest

16.79 There was some support for the use of secrecy provisions as a relevant consideration in balancing the public interest in disclosure of documents under FOI.[124] Fraser, however, expressed 'strong doubts' about the proposal:

> In the current state of specific secrecy provisions, it would not be safe to assume that the application to information of a secrecy provision, most of which are acknowledged to be extremely broad in formulation, indicates that the harm factor in an exemption is more likely to be met.[125]

Schedule 3 should be regularly reviewed and updated

16.80 The ATO advised that regular review and updating of secrecy provisions in sch 3 was its 'preferred option', and would overcome many of the practical difficulties that it currently experiences with the secrecy exemption.[126] The Treasury agreed that the provisions contained in the secrecy exemption should 'of course' be regularly reviewed and updated.[127]

16.81 The SSAT supported the regular review and updating of secrecy provisions in the secrecy exemption and recommended that agencies should have to justify their inclusion in sch 3—for example, on 'public interest' grounds.[128] Fraser also focused on the potential for ongoing justification for including a secrecy provision in the secrecy exemption. Factors that may indicate a need to remove a provision from the exemption include the omission of an express harm requirement, or substantial replication of the general secrecy offence.[129]

ALRC's views

The secrecy exemption

16.82 Two competing views were evident in submissions. On the one hand, there was support for the proposal to repeal the secrecy exemption on the basis that this would promote open government, and that other exemptions in the FOI Act provided sufficient protection. On the other hand, a number of agencies were concerned that the repeal of the secrecy exemption would leave insufficient protection for their information holdings. Particular concerns were raised by regulatory agencies that handle large amounts of personal and commercial information.

---

124 Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009; Australian Taxation Office, *Submission SR 55,* 7 August 2009.

125 R Fraser, *Submission SR 78,* 21 August 2009.

126 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

127 The Treasury, *Submission SR 60,* 10 August 2009. DoHA and the IBA also supported this proposal: Department of Health and Ageing, *Submission SR 81,* 28 August 2009; Indigenous Business Australia, *Submission SR 64,* 13 August 2009.

128 Social Security Appeals Tribunal, *Submission SR 79,* 24 August 2009.

129 R Fraser, *Submission SR 78,* 21 August 2009.

16.83 The ALRC has considered the secrecy provisions that currently invoke the exemption, and is persuaded that the exemption has an ongoing role to play. Particularly compelling in this regard are secrecy provisions which apply to a confined class of highly sensitive Commonwealth information—such as those included in the *Civil Aviation Act 1988* (Cth) and *Telecommunications (Interception and Access) Act 1979* (Cth). As set out in the Queensland Government's response to the Solomon Committee report, these matters 'require an absolute guarantee of confidentiality to ensure upfront public confidence and participation in certain processes of government'.[130]

16.84 The recommendation that the exemption should be retained also recognises the fact that numerous other recommendations in this Report seek to narrow the scope of secrecy provisions, including, in most circumstances, linking them to an express harm requirement. Implementation of these recommendations will help to minimise the potential incursion of the secrecy provision exemption on the principle of open government. However, the ALRC considers that additional reforms are needed to ensure that the exemption does not operate to reinforce a 'culture of secrecy'.

16.85 First, the secrecy exemption should be amended to include a definitive list of secrecy provisions that operate to conclusively override the FOI Act. This ensures that the minister responsible for administering the FOI Act is involved in the decision to include any secrecy provisions on the list.

16.86 Further, ministers who wish to add a secrecy provision to the list of exemptions should be required to assess, and put on the public record, the potential impact of the proposed amendment on the scrutiny of government action. Such an assessment could be included in the explanatory memorandum to ensure parliamentary scrutiny and debate. Among other considerations, relevant factors would include the breadth of the class of information to which the secrecy provision applies, and the likely relevance of the information for public scrutiny of government action.

16.87 For example, s 68 of the *Inspector of Transport Security Act 2006* (Cth), which is included in sch 3, applies to information that the Inspector has disclosed to an agency because he or she believes on reasonable grounds that:

> (a) the commission of an offence is imminent; and
>
> (b) the offence is an offence against a law of the Commonwealth, or of a State or Territory, punishable by a maximum penalty of imprisonment for more than 2 years; and
>
> (c) the information may be relevant to the prevention of the offence.

---

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

16.88 This is a far more limited class of information than that which is protected, for example, under taxation secrecy laws—which generally apply to any information about the affairs of a person collected under taxation legislation. In the ALRC's view, this is an example of a provision that would be appropriate to list in the secrecy exemption.

16.89 Another factor to be considered when including a secrecy provision in the exemption is the relevance of particular information to the scrutiny of government policies or programs. As explained in *Re Actors Equity Association of Australia and Australian Broadcasting Tribunal (No 2)*:

> To convert … commercial information into 'governmental' information and then to subject it to concepts that are in truth not appropriate to 'private' information in the commercial field would not in our view be proper, and the FOI Act makes specific provision to avoid that consequence.[131]

Interaction between the FOI Act and other secrecy provisions

16.90 There is ongoing ambiguity in relation to the interaction between exemptions in the FOI Act and secrecy provisions outside the s 38 exemption, as evident in *Kwok*. To mitigate this uncertainty, the FOI Act should be amended to expressly override a prohibition on disclosure set out in any other Act. This could be modelled, for example, on s 11 of the *Government Information (Public Access) Act 2009* (NSW). This is consistent with the ALRC's policy position that a secrecy provision should only operate as an exemption under FOI following parliamentary scrutiny, including an assessment of the implications of such an exemption for open government.

16.91 The ALRC is not recommending that the existence of a secrecy provision should be a relevant factor in assessing the public interest in making a document available under the FOI Act as proposed in DP 74. The ALRC's regulatory framework centres on the recommended general secrecy offence. This offence is based on a number of the harms identified in the FOI Act.[132] As such, it would be circular for it to be used as a relevant factor in assessing the public interest in FOI disclosure. That is, the same elements will go towards the availability of any relevant FOI exemptions categories and application of the recommended general secrecy offence.

16.92 Where a specific secrecy offence is directed at a public interest other than those recognised in the FOI Act, or protects a category of information that does not receive protection under the FOI Act, this may signal a need for reconsideration of the FOI exemptions (for example, to include information that is culturally sacred to Indigenous peoples).[133]

---

131 *Re Actors Equity Association of Australia and Australian Broadcasting Tribunal (No 2)* (1985) 7 ALD 584, 594.

132 See Ch 5.

133 The protection of Indigenous sacred and sensitive information is discussed in Ch 8.

Impact on individual officers

16.93 Individual Commonwealth officers should not be dissuaded from giving access to or publishing information in appropriate circumstances for fear of prosecution under a secrecy provision, including where disclosure is in response to an informal request or where disclosure is of 'non-sensitive exempt information'.

16.94 The ALRC affirms the recommendations in ALRC 77 that the protections against civil actions afforded by s 91 of the FOI Act should be extended to apply to authorised officers who disclose a non-exempt document other than under the FOI Act; or who disclose an exempt document pursuant to a bona fide exercise of discretion not to claim the exemption. Equivalent extensions should also apply in the context of protection from criminal prosecution. This approach has been taken in the FOI Exposure Draft Bill.

16.95 The exceptions set out in secrecy provisions indicate the circumstances in which it is appropriate for an officer to disclose information. Normally, disclosure by an authorised FOI officer will be covered by an exception for disclosure 'in the course of duties'. Disclosure in the course of an officer's duties is an exception to the recommended general secrecy offence. In Chapter 10, the ALRC considers the interaction between specific secrecy offences that do not include an exception for disclosures in the course of an officer's duties and disclosure for the purpose of other laws, such as the FOI Act.

Recommendation 16–1 Section 38 of the *Freedom of Information Act 1982* (Cth) should be amended to include a definitive list of secrecy provisions that provide an exemption from the requirement to disclose documents under the Act.

Recommendation 16–2 When it is proposed to add a secrecy provision to the revised s 38 of the *Freedom of Information Act 1982* (Cth), the explanatory memorandum for the amending legislation should provide an assessment of the potential implications for open government, including:

(a) the breadth of the class of information to which the secrecy provision applies; and

(b) the likely significance for public scrutiny of government action.

Recommendation 16–3 Sections 91 and 92 of the *Freedom of Information Act 1982* (Cth) (FOI Act) should be amended to extend the indemnities from civil and criminal actions to authorised FOI officers who:

(a) disclose an exempt document under the FOI Act pursuant to a bona fide exercise of discretion not to claim the exemption; or

(b) disclose a document other than under the FOI Act provided that:

(i) the document would not have been exempt had it been requested under the FOI Act; or

(ii) the disclosure would have been a bona fide exercise of discretion not to claim an exemption had it been requested under the FOI Act.

Recommendation 16–4 The *Freedom of Information Act 1982* (Cth) should be amended to expressly override obligations of non-disclosure in other legislation.

Archives

Overview of the *Archives Act 1983* (Cth).

16.96 The *Archives Act* establishes the National Archives of Australia (National Archives) and sets out comprehensive arrangements for conserving and preserving the archival resources of the Commonwealth.[134] The *Archives Act* was introduced at the same time as the FOI Act, as part of a package of administrative law reforms in the early 1980s. As noted in ALRC 77, the role of the National Archives includes:

> encouraging and facilitating the use of archives, developing policy and advice for government agencies on the management, preservation and disposal of records and creating and maintaining information systems about the structure of government and the Commonwealth's record series.[135]

16.97 National Archives is responsible for providing public access to government records that are in the 'open access period'. The majority of records reach the open access period after they have been in existence for 30 years.[136] A longer period of time applies to certain categories of record, including Cabinet notebooks[137] and census information.[138]

16.98 Not all Commonwealth records are retained until the open access period. Under pt V div 2 of the *Archives Act*, records can be disposed of as required by law, in

134 *Archives Act 1983* (Cth) pt V.

135 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].

136 Under proposed amendments in the FOI Exposure Draft Bill, this would be reduced to 20 years: Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth), sch 3 pt 1.

137 Currently 50 years: *Archives Act 1983* (Cth) s 22A. Under proposed amendments in the FOI Exposure Draft Bill, this would be reduced to 30 years: Exposure Draft, Freedom of Information Amendment (Reform) Bill 2009 (Cth) sch 3 pt 1.

138 Currently 99 years: *Archives Act 1983* (Cth) s 22B.

accordance with 'normal administrative practice', with the express permission of National Archives, or in accordance with a practice or procedure approved by the National Archives.

Exemptions

16.99 Section 33 of the *Archives Act* specifies a series of exemption categories, which define the types of information that may be considered to be sensitive and warrant non-disclosure in the open access period. Exemption categories include, for example, information that:

- could reasonably be expected to cause damage to the security, defence or international relations of the Commonwealth;[139]
- is communicated in confidence by or on behalf of a foreign government;[140]
- if disclosed, would, or could reasonably be expected to, prejudice the investigation of a breach of the law or prejudice the fair trial of a person;[141]
- would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person);[142] and
- is the subject of taxation secrecy provisions.[143]

16.100 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 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, those expressions arguably convey similar meanings to those discussed ... in relation to freedom of information laws.[144]

16.101 The exemption provisions set out in the federal *Archives Act* are unusual as compared with public records laws in other jurisdictions. For example, the *State Records Act 1998* (NSW) does not contain any exemption provision or enforceable access rights. New South Wales Government (NSW) agencies have discretion as to whether records should be placed in open or closed access. In Victoria, the decision as

---

139 Ibid s 33(1)(a).
140 Ibid s 33(1)(b).
141 Ibid s 33(1)(e)(i), (f)(i).
142 Ibid s 33(1)(g).
143 Ibid s 33(3). The taxation exemption is considered further below.
144 M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [5.59].

to closed or open access is at the discretion of the minister responsible for the *Public Records Act 1973* (Vic).[145]

Information covered by taxation secrecy provisions

16.102 The *Archives Act* does not have a provision equivalent to s 38 of the FOI Act. The only exemption that refers to secrecy provisions concerns taxation secrecy provisions 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.[146]

16.103 In the 1998 Report, *Australia's Federal Record: A Review of Archives Act 1983* (ALRC 85), the ALRC recommended the repeal of the exemption for information that is the subject of taxation secrecy provisions.[147] Although it recognised concerns expressed by the ATO and others about the need to protect confidentiality, the ALRC was not convinced that extra protection for these records was required in the open period:

> Most of the records of concern in this provision are routinely destroyed before they reach 30 years of age. For those records which are not destroyed, the Commission considered that any information with continuing sensitivity would be adequately protected by other exemption categories, including the information given in confidence, personal information and business affairs exemptions.[148]

16.104 The destruction of records held by the ATO is governed by *Records Disposal Authority No 1194*, issued under s 24(2)(b) of the *Archives Act*. The authority specifies various periods after which different types of records can be disposed of. Most are considerably shorter than the 30 years it takes to reach the open access period—for example, tax return forms can be destroyed after four years, and principal accounting records after seven years. A small number of records must be retained permanently.

---

145 Ibid, [5.59]–[5.63]. The *Terrorism (Community Protection) (Further Amendment) Act 2006* (Vic) has somewhat changed this situation, by inserting into the *Public Records Act* a new s 10AA. This section allows the responsible minister or the public records office to declare that a record must not be made available for public inspection in certain security and defence-related circumstances.

146 *Archives Act 1983* (Cth) s 33(3).

147 Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Rec 167. This recommendation has not been implemented.

148 Ibid, [20.77].

However, these appear to relate predominantly to high-level policy documents. With respect to cases that set precedent (which must be retained permanently), the authority specifies they must contain 'no specific reference to a client'.[149]

Census information

16.105 Officers of National Archives are themselves subject to an express secrecy provision in relation to census information. Section 30A(1) of the *Archives Act*, introduced through the *Census Information Legislation Amendment Act 2000* (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).

16.106 Section 30A(3) ensures that this provision prevails over s 58, which would otherwise allow National Archives to disclose census information where it was proper to do so or required by law.

Submissions and consultations

16.107 In response to IP 34, a number of stakeholders addressed the relationship between secrecy provisions and exemptions to the access requirements in the *Archives Act*. The Australian Bureau of Statistics and the ATO strongly defended the retention of specific exemptions with respect to their areas of operation.[150] In contrast, National Archives supported the removal of s 33(3) of the *Archives Act*, and argued that secrecy provisions in other legislation should not extend protection to open access period records.[151]

16.108 In DP 74, the ALRC affirmed the recommendation in ALRC 85 that s 33(3) of the *Archives Act* should be repealed.[152] Stakeholders expressed divided views.

16.109 The Treasury did not support repeal of s 33(3), submitting that this provision 'give[s] effect to the legitimate expectations of taxpayers that the confidentiality of their tax information will be respected, both when they provide it and in 30 years from that time'. Reliance on other exemptions in the *Archives Act* would introduce 'an element of uncertainty', that may adversely impact on taxpayer confidence.[153] Similar arguments were put forward by the ATO, which also noted that:

---

149 National Archives of Australia, *Records Disposal Authority No 1194—Australian Taxation Office* (1995).

150 Australian Bureau of Statistics, *Submission SR 28,* 24 March 2009; Australian Taxation Office, *Submission SR 13,* 16 February 2009.

151 National Archives of Australia, *Submission SR 29,* 23 February 2009.

152 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 4–5.

153 The Treasury, *Submission SR 60,* 10 August 2009.

> the repeal of s 33(3) would create an anomalous situation, where the [National Archives] could permit access to taxpayer records after 30, or possibly 20, years in circumstances where it would be a criminal offence for a tax officer to disclose those records.[154]

16.110 The Australian Transaction Reports and Analysis Centre was also concerned that repeal of s 33(3) could allow disclosure of information obtained under s 16 of the *Financial Transaction Reports Act 1988* (Cth) and ss 41 and 49 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth).[155]

16.111 Civil liberties groups supported the proposal to repeal s 33(3).[156] National Archives also supported the proposal, on the basis that exemption categories in the *Archives Act* already contain 'robust protection'. Assessing information against the exemption categories in s 33 allows determination of

> 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.[157]

16.112 IBA also supported this proposal.[158]

ALRC's views

16.113 The *Archives Act* and FOI Act mirror each other in many respects, including in a number of the exemption provisions. However, the *Archives Act* operates in a significantly different context—in particular, through the diminished sensitivity of information over time and the historical interest in information being made available during the open access period. This difference is highlighted by the small number of exemptions that apply to the disclosure of open access documents in most other jurisdictions, as discussed above.

16.114 In the ALRC's view, the taxation secrecy provision set out in s 33(3) of the *Archives Act* should be repealed. In keeping with the objective of the *Archives Act* to provide public access to government documents, this information should be made available subject to a case-by-case analysis under the other *Archives Act* exemptions. The ALRC does not anticipate that this recommendation will unduly impact on the regulatory role of the ATO, due to the routine destruction of most personal taxation information prior to the open access period and the diminished sensitivity of information by the time of open access. Remaining exemptions in the *Archives Act*,

---

154 Australian Taxation Office, *Submission SR 55,* 7 August 2009.

155 Australian Transaction Reports and Analysis Centre, *Submission SR 73,* 17 August 2009.

156 Liberty Victoria, *Submission SR 50,* 5 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009.

157 National Archives of Australia, *Submission SR 63,* 12 August 2009.

158 Indigenous Business Australia, *Submission SR 64,* 13 August 2009. The Department of Human Services agreed the relationship between secrecy provisions and the *Archives Act* should be clarified but did not express a view on the appropriate solution: Department of Human Services, *Submission SR 83,* 8 September 2009.

including those for personal privacy or where disclosure would constitute a breach of confidence, provide further protection.

16.115 The ALRC is not recommending reform of the secrecy provision in the *Archives Act* in relation to census information. The provision only applies to census information prior to its entry into the open access period, as compared with the tax secrecy exemption which applies indefinitely. Further, the assurance of absolute secrecy for the designated time—currently 99 years—enhances the Australian archival system by ensuring public confidence in providing identified census information to the National Archives.

Recommendation 16–5 Section 33(3) of the *Archives Act 1983* (Cth) should be repealed.

Interaction between the *Archives Act* and other secrecy provisions

16.116 With the exception of census and tax information, discussed above, the *Archives Act* does not make reference to secrecy provisions in other Acts. This has given rise to some uncertainty about the relationship between secrecy requirements and the public access provisions of the *Archives Act*.[159] National Archives advised that it has sought legal advice on five occasions between 1985 and 1998 to confirm that the *Archives Act* has primacy over confidentiality or secrecy provisions in a number of other Acts.[160] It suggested that the relationship between secrecy provisions and the *Archives Act* could be clarified:

> 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.[161]

16.117 In ALRC 85, it was noted that the 1979 draft of the Archives Bill included a clause which provided for a schedule of enactments which would override the access provisions of the archives legislation. In reviewing the Bill, the Senate Standing Committee on Constitutional and Legal Affairs 'strongly opposed' inclusion of the provision on the basis that 'a possible conflict of obligations would not … justify or

159 Several instances where conflict has arisen were canvassed in Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998) [15.58]–[15.61].
160 National Archives of Australia, *Submission SR 29,* 23 February 2009.
161 Ibid.

necessitate the exclusion of some categories of records from the access provisions'.[162] The provision was subsequently removed from the Bill.[163]

16.118 The ALRC recommended that the *Archives Act* should

> expressly provide 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.[164]

16.119 This reflects the position, for example, under s 53 of the *State Records Act 1998* (NSW), which provides that secrecy provisions do not apply to disclosure of information in the open access period. The section 'does not apply to a provision of an Act if the Act provides specifically to the effect that the prohibition concerned applies despite this Act', or where a specified provision of an Act is exempted from the operation of the section under the regulations.[165]

Submissions and consultations

16.120 In DP 74, the ALRC proposed that the *Archives Act* should provide 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.[166] In order to effect this reform, the ALRC proposed that 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* in the open access period.[167]

16.121 Several government and other stakeholders supported the proposed inclusion of an override provision in the *Archives Act* and a corresponding drafting direction.[168] However, National Archives raised concerns about the potential for other legislation to expressly override the *Archives Act*—in particular, that this could have the effect of excluding records from the access and review provisions of the *Archives Act*. National Archives suggested that such an override could require a new exemption category in

---

162 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), [33.28].

163 Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), [15.62].

164 Ibid, Rec 108.

165 At the time of writing, no secrecy provisions were exempted from the operation of s 53 of the *State Records Act 1998* (NSW) under the *State Records Regulations 2005* (NSW).

166 Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009), Proposal 4–6.

167 Ibid, Proposal 4–7.

168 See, eg, Indigenous Business Australia, *Submission SR 64,* 13 August 2009; National Archives of Australia, *Submission SR 63,* 12 August 2009; Civil Liberties Australia, *Submission SR 47,* 27 July 2009. The Department of Human Services agreed the relationship between secrecy provisions and the *Archives Act* should be clarified but did not express a view on the appropriate solution: Department of Human Services, *Submission SR 83,* 8 September 2009.

s 33, which refers to records that are subject to a non-disclosure provision in another Act.[169]

16.122 National Archives expressed in-principle support for the proposed drafting direction, 'insofar as it is necessary to provide for another Act to override the *Archives Act*'. National Archives reiterated its preferred position, however, that secrecy provisions in other Acts should lapse when records reach the open access period. Further, if a non-disclosure provision is applied to records in the open-access period, then the exemption should be included in the *Archives Act*. This would 'clearly identify the limits to the right of access and make sure that decision makers and applicants are aware of all non-disclosure provisions'.[170]

16.123 The ATO opposed the proposed override provision on the basis that it could undermine the protection provided to taxpayer information and create uncertainty for tax officers. However, it expressed support for the proposed drafting direction. The ATO advised that, should s 33(3) of the *Archives Act* be repealed and the time to reach the open access period reduced to 20 years (as is proposed in the FOI Exposure Draft Bill), the taxation secrecy provision will need to be updated to ensure taxpayer information retains sufficient protection.[171]

ALRC's views

16.124 To overcome any real or perceived ambiguity, the *Archives Act* should provide that the public access provisions of the Act override any secrecy provisions that would otherwise apply. This is consistent with the ALRC's recommendations in ALRC 85 and its proposal for reform in DP 74.

16.125 It is important to note that the ALRC is not, however, recommending that legislation should be drafted to expressly override the open access provisions in the *Archives Act*. For the reasons set out in support of Recommendation 16–5, the ALRC is not aware of any secrecy provisions that warrant categorical exemption from the open access provisions of the *Archives Act*. This was also the view of the Senate Standing Committee on Constitutional and Legal Affairs in its 1979 report.[172]

16.126 In the event that a future Parliament is of the view that a secrecy provision should form the basis of an exemption from the open access requirements of the *Archives Act*, the exemption should be included in the *Archives Act* itself. As submitted by National Archives, this will provide clarity for decision makers, as well as ensuring that those seeking access to such records will have recourse to the avenues set out in the *Archives Act* for review of decisions.

---

169 National Archives of Australia, *Submission SR 63,* 12 August 2009.
170 Ibid.
171 Australian Taxation Office, *Submission SR 55,* 7 August 2009.
172 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), [33.28].

Recommendation 16–6 The *Archives Act 1983* (Cth) should be amended to provide that the public access provisions of the Act override any secrecy provisions that would otherwise apply.

Privacy

Overview of the *Privacy Act 1988* (Cth)

16.127 The *Privacy Act* aims to protect personal information and to give individuals some control over how such information is handled. In contrast to secrecy provisions—which predominantly regulate individuals, for example, Commonwealth officers—the *Privacy Act* imposes obligations on both public sector agencies and private organisations, as defined in the Act.[173]

16.128 The requirements of the *Privacy Act* are largely set out in two sets of privacy principles—the Information Privacy Principles (IPPs) and National Privacy Principles (NPPs). These provide a primarily principles-based framework for the manner in which Australian Government agencies[174] and private sector organisations, respectively, can collect, store, use and disclose personal information.[175] They also give individuals rights of access to, and correction of, their own personal information.

16.129 The privacy principles, and other requirements of the *Privacy Act*, only apply insofar as an agency or organisation is handling 'personal information', 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.[176]

16.130 In 2008, the ALRC released the report, *For Your Information: Australian Privacy Law and Practice* (ALRC 108),[177] including 295 recommendations for the reform of privacy laws and practices. Most relevantly to this Inquiry, the ALRC recommended that there should be: a uniform set of privacy principles to apply to all

---

173 Note, however, that under the Australian Public Service (APS) Code of Conduct, APS employees are required to comply with all applicable Australian laws: *Public Service Act 1999* (Cth) s 13(4). This would include compliance with the *Privacy Act 1988* (Cth).

174 Note, however, that the acts and practices of some Australian Government agencies—including the intelligence agencies ASIS, ASIO and the Office of National Assessments—are completely exempt from the operation of the *Privacy Act*: *Privacy Act 1988* (Cth) s 7.

175 Ibid s 14 (IPPs), sch 3 (NPPs).

176 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.

177 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008).

federal government agencies and the private sector; rationalisation of exemptions and exceptions to *Privacy Act* requirements; improved complaint-handling procedures; and stronger penalties for breach. On 14 October 2009, the Australian Government released its response to 197 of the recommendations in ALRC 108. It accepted the vast majority of these recommendations, including that there should be a uniform set of privacy principles.[178]

Interaction between the *Privacy Act* and secrecy provisions

16.131 Protection of private personal and commercial information has frequently been a driving factor in the enactment of secrecy laws. The current diversity of secrecy provisions has been attributed to the greatly increased collection of personal and commercially sensitive information by the government since the mid-1940s, in areas such as taxation, health and welfare.[179] As noted in Chapter 3, approximately one third of secrecy provisions specifically protect personal information.

16.132 The role of secrecy laws in protecting personal information was particularly apparent in the era prior to the enactment of the *Privacy Act*. However, many secrecy provisions enacted more recently continue to emphasise the importance of secrecy laws operating alongside the *Privacy Act*. Secrecy provisions in the context of taxation information are a clear illustration. For example, the explanatory memorandum accompanying the Inspector-General of Taxation Bill 2003 (Cth) states that the secrecy provision in cl 23 was drafted, not only to mirror secrecy provisions across tax law, but also 'to be consistent with privacy laws'.[180] Similar objectives have been expressed in the area of health information, with the secrecy provision in the *Australian Organ and Tissue Donation and Transplantation Authority Act 2008* (Cth) designed 'as an additional safeguard' to operate in tandem with the *Privacy Act.*[181]

16.133 A different interaction between secrecy provisions and the *Privacy Act* takes place where secrecy provisions are used to facilitate information sharing, which—outside the legislative authorisation provided by a secrecy provision—would be impermissible under the *Privacy Act*. This issue is particularly relevant in the context of whole of government policies and programs, which are becoming an increasingly prevalent feature of modern government.[182]

---

178 The Australian Government accepted 141 of the 197 recommendations in full or in principle, with another 34 recommendations accepted with qualification and two further recommendations noted (but not requiring action): Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

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

180 Explanatory Memorandum, Inspector General of Taxation Bill 2002 (Cth).

181 Explanatory Memorandum, Australian Organ and Tissue Donation and Transplantation Authority Bill 2008 (Cth).

182 The move to open government is discussed in Ch 2.

16.134 The only part of the *Privacy Act* that addresses the interaction with secrecy provisions is pt VIA,[183] which provides for the handling of personal information in emergencies or disasters. In this part, s 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).[184]

16.135 The following discussion focuses on issues raised where information is subject to both information-handling requirements under the *Privacy Act* and secrecy provisions. These include ambiguities that may result from the use of inconsistent terminology in privacy and secrecy laws, and the application of secrecy provisions to lessen the minimum standards set out in the privacy principles.

Terminology

16.136 As noted above, a large number of secrecy provisions apply to information about individuals. In a small number of situations, secrecy provisions expressly or impliedly mirror the definition of personal information in the *Privacy Act*. Section 16 of the *Customs Administration Act 1985* (Cth), for example, defines personal information as having the same meaning as that set out in the *Privacy Act*.[185] Section 86-2(1) of the *Aged Care Act* defines personal information in identical terms to the *Privacy Act,* but without reference to that Act.[186]

16.137 However, other provisions use a variety of formulations. For example, s 30 of the *A New Tax System (Australian Business Number) Act 1999* (Cth) protects information that 'relates to the affairs of a person other than the entrusted person'.[187] The term 'affairs of a person' is used in more than 50 other secrecy provisions, which both pre-date[188] and post-date[189] enactment of the *Privacy Act*. Secrecy provisions directed to the protection of information held by health and welfare agencies

---

183 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.

184 *Privacy Act 1988* (Cth) s 80P(7).

185 *Customs Administration Act 1985* (Cth) s 16(1A), 16(7). See also *Air Navigation (Confidential Reporting) Regulations 2006* (Cth) reg 14.

186 *Aged Care Act 1997* (Cth) sch 3.

187 *A New Tax System (Australian Business Number) Act 1999* (Cth) s 41. 'Protected information' also must be: obtained by the entrusted person (or any person) in the course of official employment; and disclosed or obtained under the Act. Section 41 also provides that a 'person' includes a company, and s 30(1) provides that an 'entrusted person' is a person that has obtained protected information in the course of official employment.

188 For example, *Australian Trade Commission Act 1985* (Cth) s 94; *Health Insurance Act 1973* (Cth) s 130.

189 For example, *Aboriginal and Torres Strait Islander Act 2005* (Cth) ss 191, 200A;*Inspector-General of Taxation Act 2003* (Cth) s 37.

commonly protect information 'about' or 'concerning' a person'.[190] Approximately 30 secrecy provisions prevent the disclosure of information only where it could identify a person. For example, s 323 of the *Commonwealth Electoral Act 1918* (Cth) prohibits the disclosure of information that is 'likely to enable the identification of the elector'.

16.138 Quite different meanings attach to the above formulations. For example, in *Young v Wicks*, 'personal affairs' was interpreted as 'matters of private concern to a person'.[191] Since the relevant factor is the nature of the information, the 'personal affairs' criterion might be satisfied even where any matters which could identify a person have been removed.[192] In comparison, the definition of 'personal information' under the *Privacy Act*[193] focuses on whether an individual's identity is clear, or reasonably capable of being ascertained, from the information.

16.139 The *Acts Interpretation Act 1901* (Cth) provides that the word 'person' includes a body politic or corporate as well as an individual.[194] Where a secrecy provision regulates the handling of information that, for example, relates to the 'affairs of a person', this may extend to information related to a corporate or political entity as well as an individual.

Minimum standards of privacy protection

16.140 The IPPs and the NPPs set out baseline standards with which agencies and organisations must comply in their handling of personal information. As explained by the Office of the Privacy Commissioner in the context of IPPs 8 to 11:

> **IPPs only set out minimum standards**
>
> The IPPs only set out minimum legal standards for agencies in dealing with personal information. A higher standard may be appropriate, even if the IPPs do not require it.
>
> It may be appropriate for an agency to take more care to protect people's privacy (than the IPPs require) if:
>
> (a) particularly sensitive personal information is involved, or
>
> (b) using or disclosing personal information is likely to have serious consequences for the person the information is about.[195]

---

190 For example, *Child Support (Registration and Collection) Act 1988* (Cth) ss 16, 16AA; *Health Insurance Act 1973* (Cth) s 130; *National Health Act 1953* (Cth) s 135A.

191 *Young v Wicks* (1986) 13 FCR 85. See also *Commissioner of Police v District Court of New South Wales* (1993) NSWLR 606, 625; *Colakovski v Australian Telecommunications Corporation* (1991) 29 FCR 429, 436; *Re F and Health Department* (1988) 2 VAR 458, 461.

192 This issue is discussed in the context of the operation of the secrecy provision exemption in the FOI Act in Australian Government Solicitor, *FOI Guidelines—Exemption Sections in the FOI Act* (2009) <www.dpmc.gov.au> at 9 September 2009, [9.1.8]–[9.1.9].

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

194 *Acts Interpretation Act 1901* (Cth) s 22.

195 Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles 8–11* (1996) <www.privacy.gov.au> at 7 October 2009, 6–7.

16.141 However, through exceptions in the IPPs and NPPs for acts or practices 'required or authorised by or under law', secrecy provisions may lower standards of privacy protection by allowing information-handling practices that are not expressly permitted in the privacy principles—most notably, in the principles in relation to access and correction and disclosure.

Access and Correction

16.142 IPP 6, 'Access to records containing personal information', provides an individual with the right to access personal information that an agency holds about him or her

> except to the extent that the record−keeper is required or authorised to refuse to provide the individual with access to that record under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

16.143 Many secrecy provisions reflect the idea that individuals should generally have access to information held about them by public authorities. For example, s 86-2 of the *Aged Care Act* creates an offence for the unauthorised handling of 'protected information'. However, the section contains an exception for information disclosed 'only to the person to whom it relates'.[196] A further illustration is s 94 of the *Australian Trade Commission Act 1985* (Cth), which restricts the disclosure 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'. By limiting the prohibition to information of 'another' person, disclosure appears to be permitted to the person to whom the information relates.

16.144 In contrast, however, 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'.[197] 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, none of these are equivalent to the exception contained in s 86-2 of the *Aged Care Act.*

Disclosure

16.145 IPP 11.1 sets out a general prohibition on the disclosure of personal information by government agencies other than in limited circumstances. Permissible secondary disclosures include where:

---

196 *Aged Care Act 1997* (Cth) s 86-2(2)(b).

197 *Surveillance Devices Act 2004* (Cth) s 44(3) also prohibits the admission of protected information in evidence in any court proceedings.

> (a) the individual concerned is reasonably likely to have been aware, or made aware under [the Collection principle], that information of that kind is usually passed to that person, body or agency;
>
> (b) the individual concerned has consented to the disclosure;
>
> (c) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person;
>
> (d) the disclosure is required or authorised by or under law; or
>
> (e) the disclosure 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.

16.146 Exceptions to the prohibition on non-disclosure in secrecy provisions will often invoke IPP 11.1(d)—the 'required or authorised by or under law' exception. For example, s 56 of the *Australian Prudential Regulation Authority Act 1998* (Cth) prohibits the disclosure of protected information (including personal information) except in specific circumstances. These include, for example, where the disclosure is approved by APRA in writing, or is to an APRA member or staff member 'for the purpose of the performance of APRA's functions or the exercise of APRA's powers, under a law of the Commonwealth or of a State or a Territory'. Section 56(12) makes clear that:

> A disclosure of personal information is taken to be authorised by law for the purposes of paragraph (1)(d) of Information Privacy Principle 11 in section 14 of the *Privacy Act 1988* if:
>
> (a) the information is protected information and the disclosure is made in accordance with any of subsections (4), (5), (5AA), (6), (7A), (7B) and (7C); or
>
> (b) the information is contained in a protected document and the disclosure is made by the production of the document in accordance with any of those subsections.

Options for reform in ALRC 108

16.147 In ALRC 108, the ALRC considered possible reforms to deal with the overlap between privacy and secrecy laws, including whether the *Privacy Act*—rather than specific secrecy provisions—should regulate the disclosure of personal information by Australian government agencies. The ALRC did not recommend such a reform. First, retaining secrecy provisions in specific statutes 'ensures that an agency's secrecy responsibilities are tailored to the agency's circumstances and grouped with other obligations'.[198] Secondly:

> 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

198 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [15.120].

> privacy principles … Unlike the privacy principles, the level of protection afforded by secrecy provisions will often vary with the sensitivity of the information concerned.[199]

16.148 Given that secrecy provisions may adversely affect the privacy of an individual, however, the ALRC considered the use of privacy impact assessments (PIA) in this context.

16.149 A PIA has been described as 'an assessment of any actual or potential effects that [an] activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated'.[200] Currently, there are no requirements in the *Privacy Act* for an agency to undertake a PIA. However, the Office of the Privacy Commissioner has published a *Privacy Impact Assessment Guide*, which recommends that agencies undertake a PIA as part of their advice on certain legislative proposals and policy submissions.[201]

16.150 In ALRC 108, the ALRC recommended that the Privacy Commissioner should be empowered under the *Privacy Act* to direct an agency to provide a PIA 'in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information'.[202] Consistently with this recommendation, the ALRC expressed the view that a PIA should be prepared when a secrecy provision is proposed that may have a significant impact on the handling of personal information.[203]

16.151 The ALRC also suggested that, where a secrecy provision regulates personal information, it should address how the requirements under the provision interact with the privacy principles.[204]

Submissions and consultations

16.152 In IP 34, the ALRC sought views on the relationship between secrecy provisions and the *Privacy Act*. In particular, the ALRC questioned whether secrecy

---

199 Ibid, [15.121].

200 Ibid, [47.44], citing B Stewart, 'Privacy Impact Assessments' (1996) 3 *Privacy Law and Policy Reporter* 61, 62. Privacy impact assessments are discussed in detail in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Ch 47.

201 Office of the Privacy Commissioner, *Privacy Impact Assessment Guide* (2006) <www.privacy.gov.au> at 7 October 2009.

202 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 47–4. This proposal was limited to agencies; however, the ALRC further recommended that a review be undertaken five years after the amendment is introduced to consider expansion to the private sector: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 47–5. The Australian Government has accepted Recs 47–4 and 47–5: Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

203 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [15.122]–[15.124].

204 Ibid.

provisions should regulate personal information and, if so, whether they should refer to or use the terminology of the *Privacy Act*[205] and allow individuals to access and correct personal information about themselves.[206] Finally, the ALRC asked whether there were situations in which it was appropriate for secrecy provisions to authorise a lower standard of privacy protection than would be permissible under the *Privacy Act*.[207]

Overlap between secrecy and privacy laws

16.153 A number of stakeholders noted the complementary nature of secrecy and privacy laws, and the need to retain both of these regimes to regulate the disclosure of personal information effectively.[208] As stated in the submission of the Office of the Privacy Commissioner:

> the *Privacy Act* provides an overarching framework for how personal information should be handled by an agency and this framework is complemented by information type or agency specific secrecy provisions which address where the agency needs to protect the confidentiality of personal information as they carry out their particular activities and functions.[209]

16.154 The Office expressed the view that:

> secrecy provisions should continue to regulate personal information in circumstances where a need has been identified for that information to be subject to additional confidentiality protections or specific handling requirements over and above those afforded by the *Privacy Act*.[210]

16.155 The Office also recognised that secrecy provisions may apply to an array of Commonwealth information, of which personal information is a subset:

> To establish a situation where the handling of a portion of the information contained in a record is regulated by a secrecy provision and the handling of personal information in other parts of the same record is regulated exclusively by the *Privacy Act* could result in confusion and inconsistency in the application of both the laws. For example, trying to delineate information relating to the taxation matters of a small business and its owner would be impractical and could prove very difficult in determining what information is regulated by the *Privacy Act* and what is regulated by a secrecy provision.[211]

16.156 In a submission in response to DP 74, the Office of the Privacy Commissioner suggested that the 'uncertainty regarding the intersection of obligations imposed by both pieces of legislation' could be lessened by adopting a drafting

---

205 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 7–4(a).
206 Ibid, Question 7–4(b).
207 Ibid, Question 7–5.
208 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009; Attorney-General's Department, *Submission SR 36,* 6 March 2009; Australia's Right to Know, *Submission SR 35,* 6 March 2009; Australian Taxation Office, *Submission SR 13,* 16 February 2009.
209 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009.
210 Ibid.
211 Ibid.

direction requiring any proposed secrecy provision that will regulate the handling of personal information to indicate expressly how it will interact with the agency's responsibilities under the *Privacy Act*. In the view of the Office:

> Such a requirement provides a specific trigger for agencies to consider their obligations in relation to the handling of that personal information. It would also provide clarification regarding the interaction between the secrecy provision and the *Privacy Act* at the time of drafting to avoid subsequent confusion.[212]

16.157 The AGD commented favourably on the potential for secrecy provisions to regulate the disclosure of personal information in situations where the remedies available under the *Privacy Act* are not considered to have sufficient deterrent effect.[213]

16.158 Although the ARTK coalition accepted the need for secrecy provisions and the *Privacy Act* to operate concurrently, it raised concerns about the potential for agencies to use privacy as 'a shroud to the provision of information to the public'.[214] Dr Ian Turnbull also commented on detrimental consequences that may flow where the concepts of privacy and secrecy are confused, suggesting that:

> 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.[215]

16.159 In contrast, the Non-Custodial Parents Party noted the need for strong privacy protection and submitted that privacy provisions should always prevail over secrecy laws.[216]

16.160 Ron Fraser commented on the expanded role that privacy law is likely to play if there is a reduction in the number of specific secrecy provisions. This includes the provision of 'a floor below which privacy protection in relation to personal information cannot fall except with specific legal authority'.[217]

Terminology

16.161 The Office of the Privacy Commissioner expressed the view that secrecy provisions that relate to the handling of personal information should refer to or use the terminology of the *Privacy Act*, where possible:

> For example, the Office suggests that either using the *Privacy Act*'s definition of 'personal information' or making reference to the definition and specifically stating what additional information, if any, is included in the secrecy provision's scope of

---

212 Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009.
213 Attorney-General's Department, *Submission SR 36,* 6 March 2009. See also Australian Press Council, *Submission SR 16,* 18 February 2009.
214 Australia's Right to Know, *Submission SR 35,* 6 March 2009.
215 I Turnbull, *Submission SR 15,* 17 February 2009.
216 Non-Custodial Parents Party (Equal Parenting), *Submission SR 82,* 3 September 2009.
217 R Fraser, *Submission SR 78,* 21 August 2009.

> 'personal information' would help clarify the interaction between the *Privacy Act* and the secrecy provision.
>
> Alternatively, where using the *Privacy Act*'s terminology is not practical or feasible, it may be useful for secrecy provisions that relate to personal information to address how the terminology used interacts with that of the *Privacy Act*. For example, where a secrecy provision uses the term 'release' information, it would assist to note how, if at all, that differs from 'disclose' in the *Privacy Act*.[218]

16.162 The 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'.[219] The AGD also supported such consistency, noting that:

> 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*.[220]

16.163 Although the Department of Education, Employment and Workplace Relations recognised the benefits of consistent terminology, it cautioned that there would be 'little value' in a secrecy provision simply mirroring the *Privacy Act* since 'specific secrecy provisions are designed to cater for the particular context and nature of the information [that is] being regulated'.[221]

16.164 A similar issue was raised by the Department of Human Services (DHS), which submitted that secrecy provisions apply to a wider range of information than the *Privacy Act*. Adopting *Privacy Act* terminology would only be appropriate where there is an intention to restrict the coverage of secrecy laws to correlate to information protected under the *Privacy Act*.[222]

Rights to access and correction

16.165 In IP 34, the ALRC asked whether secrecy provisions should allow individuals to access and correct personal information about themselves.[223] The ATO submitted 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

---

218 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009.
219 Social Security Appeals Tribunal, *Submission SR 14,* 17 February 2009.
220 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
221 Department of Education, Employment and Workplace Relations, *Submission SR 24,* 19 February 2009.
222 Department of Human Services, *Submission SR 26,* 20 February 2009. See also Indigenous Business Australia, *Submission SR 64,* 13 August 2009.
223 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 7–4(b).

> will never apply to restrict a taxpayer from accessing his or her own tax information.[224]

16.166 A similar point was made by the DHS, which advised that the secrecy provisions applying to agencies in the human services portfolio do not raise barriers to the processes of access and correction set out in the *Privacy Act* and FOI Act.[225]

16.167 The Office of the Privacy Commissioner was of the view that the *Privacy Act*, rather than secrecy provisions, was the most appropriate avenue for individuals to obtain access to, or correction of, personal information:

> Having these individual rights expressed in the *Privacy Act* is consistent with the nature of the Act but may sit at odds with the majority of secrecy provisions as they focus on the protection of information through obligations of confidentiality or secrecy, rather than the accessibility to or quality of personal information.[226]

16.168 Further, the Office suggested that retaining access and correction provisions in the *Privacy Act*, rather than in various secrecy provisions, 'will assist in reducing fragmentation and inconsistency'. The Office suggested, however, that for agencies that are not covered by the *Privacy Act*—for example, ASIO—it might be appropriate to include any applicable access and correction provisions in relevant secrecy provisions.[227]

Permissible disclosure of personal information

16.169 In IP 34, the ALRC sought views on when it might be appropriate for a secrecy provision to authorise the handling of personal information that would otherwise breach the *Privacy Act*.[228]

16.170 The AGD suggested that legitimate reasons for authorising the handling of personal information through secrecy provisions could include, for example, for the purposes of law enforcement or the detection and prevention of fraud.[229]

16.171 From the perspective of the Office of the Privacy Commissioner, however:

> The protections afforded through the IPPs should be considered fundamental obligations that agencies should not legislate to reduce. … [S]hould an agency identify a need to handle personal information in a way that is inconsistent with or would otherwise breach the IPPs, then there needs to be a clear policy basis or public policy need for doing so.[230]

---

224 Australian Taxation Office, *Submission SR 13,* 16 February 2009.
225 Department of Human Services, *Submission SR 26,* 20 February 2009.
226 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009.
227 Ibid.
228 Australian Law Reform Commission, *Review of Secrecy Laws*, Issues Paper 34 (2008), Question 7–5.
229 Attorney-General's Department, *Submission SR 36,* 6 March 2009.
230 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009. See also Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009.

16.172 The Office raised particular concerns about the exception to obligations of agencies under several IPPs for conduct that is 'required or authorised by law':[231]

> The Office strongly believes that this exception should not be used as the basis for requiring or authorising practices that are detrimental to the individual or included without a strong policy rationale. As far as practicable, reliance on this exception should also be careful not to remove more of the baseline protections provided by the *Privacy Act* than absolutely necessary and should still reflect the spirit and intent of the Act wherever possible.[232]

16.173 Where an agency authorises activities that are potentially in conflict with its obligations under the IPPs, the Office expressed the view that the agency should complete a PIA:

> The completion of a PIA is a useful process for agencies to gain an understanding of the implications of any proposed secrecy provisions which relate to the handling of personal information. A PIA is a practical tool to assess information flows and determine whether provisions are necessary and reflective of best privacy practice. Conducting a PIA through the use of an independent specialist builds transparency into the decision making process and enhances confidence that the need for provisions has been assessed objectively. As such, the Office recommends that PIAs should be completed when either a new secrecy provision or a significant amendment to a current secrecy provision is being proposed.[233]

16.174 The DHS sought greater clarity in the application of the 'required or authorised by or under law' exception in IPP 11:

> 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).[234]

ALRC's views

16.175 Many secrecy provisions were enacted prior to the introduction of the *Privacy Act* in order to deal with what were essentially privacy concerns. In Chapter 8, the ALRC recommends that specific secrecy offences are only warranted where they are necessary and proportionate to the protection of essential public interests of

---

231 *Privacy Act 1988* (Cth) s 14 IPPs 10(c), 11(d).

232 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009. See also Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009.

233 Office of the Privacy Commissioner, *Submission SR 46,* 24 June 2009. See also Office of the Privacy Commissioner, *Submission SR 66,* 13 August 2009. The Australian Privacy Foundation also endorsed the use of PIAs. Australian Privacy Foundation, *Submission SR 71,* 16 August 2009.

234 Department of Human Services, *Submission SR 26,* 20 February 2009. See also Community and Disability Services Ministers' Advisory Council, *Submission SR 80,* 28 August 2009.

sufficient importance to justify criminal sanctions.[235] As discussed in Chapter 8, the ALRC considers that the unauthorised disclosure of personal or commercial information does not, without more, warrant criminal sanctions under specific secrecy offences, except in very limited circumstances. In these limited circumstances, personal information will be governed by both a specific secrecy offence and the *Privacy Act*.[236] In other circumstances, personal information may be regulated by a non-criminal specific secrecy provision and the *Privacy Act*.

16.176 The ALRC agrees with the comments of many stakeholders that there are benefits in having a tiered system for protecting personal information. The *Privacy Act* provides an overarching framework for the manner in which Australian Government agencies handle personal information, complemented by secrecy provisions, which focus on individuals in particular agencies, or who handle certain types of information where a greater degree of confidentiality is warranted.

16.177 Consequently, the ALRC sees two key roles for reform:

- ensuring that privacy protections are upheld to the greatest possible extent; and
- clarifying the interaction between the *Privacy Act* and secrecy provisions that apply to personal information.

Protecting personal information

16.178 Secrecy provisions can infringe on the protection of an individual's personal information by:

- removing his or her right to obtain access to, and correction of, personal information; or
- expanding the scope of permissible disclosures of personal information by requiring or authorising the sharing of certain information.

16.179 In ALRC 108, the ALRC emphasised the importance of encouraging agencies to conduct PIAs voluntarily. The ALRC further recommended that where the Privacy Commissioner considers that a new project or development would have a 'significant impact on the handling of personal information', he or she should have the power to direct an agency to prepare a PIA.[237] The ALRC remains of the view that

---

235 Recommendation 8–1.

236 The ALRC is not recommending that harm to personal privacy should form an element of the general secrecy offence: see Ch 5.

237 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Rec 47–4. This recommendation was accepted by the Australian Government. Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

PIAs provide a suitable mechanism for agencies and others to identify and consider the privacy implications of a proposed secrecy provision.

16.180 In particular, the ALRC recommends that an agency should conduct a PIA where a proposed secrecy provision would require or authorise information-handling practices that significantly detract from the standards set out in the *Privacy Act*. In the event that an agency chose not to undertake such an assessment, the Privacy Commissioner may wish to exercise his or her power of direction in this regard.

Clarity of application

16.181 Stakeholders have identified situations where it is unclear whether a secrecy provision operates as an exception to the privacy principles for acts 'required or authorised by or under law'. For example, does an exception for disclosures in the course of an officer's duties authorise the release of information under the disclosure principle in IPP 11.1?

16.182 In ALRC 108, the ALRC considered possible reforms to the operation of the 'required or authorised by or under law' exception in the *Privacy Act*, including whether provisions in federal legislation that require or authorise practices for the purpose of the *Privacy Act* should clearly refer to the exception. The ALRC stated that 'it would be too onerous to amend all existing federal, state and territory legislation that may require or authorise an act or practice relating to the handling of personal information'.[238] However, where possible, proposed laws that are intended to rely on the required or authorised exception should state this expressly.[239] The ALRC also recommended that the Office of the Privacy Commissioner should 'develop and publish guidance to clarify when an act or practice will be required or authorised by or under law'.[240]

16.183 The ALRC affirms these recommendations, and considers that these strategies would largely resolve the potential ambiguities identified in the context of the interaction between the *Privacy Act* and secrecy provisions. In Chapter 11, the ALRC recommends that Australian Government agencies should review specific secrecy offences. This review would provide an opportunity for the Australian Government to consider any interaction between a provision and the *Privacy Act*, including the need to include clear references to the exception for acts and practices required or authorised by or under law.[241] Accordingly, no further recommendations are made in this regard.

---

238 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [16.93].

239 Ibid.

240 Ibid, Rec 16–2. The Australian Government accepted this recommendation. Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

241 Recommendation 11–1.

16.184 Another source of potential ambiguity is the inconsistent use of terminology such as 'personal information', 'affairs of a person' and other similar formulations. The ALRC acknowledges the clear benefits of using the definition of personal information set out in the *Privacy Act* in secrecy provisions. The *Privacy Act* provides a comprehensive and nuanced definition of the information which warrants protection in order to satisfy personal privacy objectives.[242] Consistent terminology also provides a ready body of precedent for Commonwealth officers and others seeking to understand whether a secrecy provision applies to specific information.

16.185 However, the definition of personal information in the *Privacy Act* is only applicable to those secrecy provisions whose objects are directed towards the protection of personal privacy. A term such as 'affairs of a person' may be warranted, for example, where a secrecy provision is also intended to apply to information about commercial entities. Accordingly, the ALRC is not recommending that secrecy provisions should adopt *Privacy Act* terminology as a matter of course. Rather, this is an issue that should be considered as a part of the drafting process. The review of specific secrecy provisions recommended in Chapter 11 provides an opportunity to consider whether a secrecy provision that regulates personal information should adopt the *Privacy Act* definitions.

Recommendation 16–7 The Australian Government should conduct a Privacy Impact Assessment for a proposed secrecy provision that would require or authorise information-handling practices that significantly detract from the standards set out in the *Privacy Act 1988* (Cth).

Parliamentary privilege

Background

16.186 In response to IP 34, the Clerk of the Senate, Harry Evans, provided a submission to draw to the ALRC's attention an issue that arises from the relationship between secrecy provisions and the operation of parliamentary privilege:

> From time to time executive government officials suggest that statutory secrecy provisions prevent them providing information to either House of the Parliament or its

242 In Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), the ALRC made several recommendations for reform of the definition of 'personal information' in the *Privacy Act*: Recs 6–1 to 6–3. The Australian Government accepted these recommendations. Australian Government, *Enhancing National Privacy Protection—Australian Government First Stage Response to the Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice* (2009).

> committees and/or render them liable under such provisions for supplying relevant information.[243]

16.187 Evans 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'.[244]

What is parliamentary privilege?

16.188 '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.[245] 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.

16.189 The importance of parliamentary privilege is clearly set out in the *Human Rights Handbook for Parliamentarians* prepared for the United Nations by Manfred Nowak:

> Parliament can fulfil its role only if its members enjoy the freedom of expression necessary in order to be able to speak out on behalf of constituents. Members of parliament must be free to seek, receive and impart information and ideas without fear of reprisal. They are therefore generally granted a special status, intended to provide them with the requisite independence: they enjoy parliamentary privilege or parliamentary immunities.[246]

16.190 There are two aspects of parliamentary privilege. The first is set out in art 9 of the *Bill of Rights 1688* (UK) (applied in Australia by virtue of s 49 of the *Australian 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 amount to '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.

---

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

244 Clerk of the Senate, *Submission SR 03,* 23 January 2009.

245 H Evans (ed), *Odgers' Australian Senate Practice* (12th ed, 2008), Ch 2.

246 M Nowak, *Human Rights Handbook for Parliamentarians* (2005), 64.

16.191 On this basis, the Parliament, or a parliamentary committee, generally has the power to compel the giving of evidence or the production of documents that otherwise would be covered by a secrecy provision. In this context, a person who discloses information will be immune from liability under any secrecy provision.

Express abrogation of parliamentary privilege

16.192 Parliament may choose to abrogate parliamentary privilege expressly and prevent the disclosure of information to the Parliament or its committees.[247] 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' certain information 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'.[248]

16.193 A far more detailed regime for dealing with disclosures to ministers and parliament is included in the Exposure Draft of the Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) (Tax Laws Exposure Draft Bill). The draft Bill sets out an exhaustive list of permissible disclosures to ministers and parliamentary committees.[249] These include, for example, disclosure to any minister to enable him or her to exercise a power or perform a function under a taxation law; and disclosure to the Treasurer for the purpose of enabling him or her to respond to an entity's representation.

16.194 The Tax Laws Exposure Draft Bill makes clear that the disclosures listed in the Bill are the only permissible disclosures that an officer can make to ministers and parliament, 'despite any power, privilege or immunity of either House of the Parliament or members or committees of either House of Parliament'.[250] However, the Bill retains the Parliament's powers of compulsion, and authorises an officer to disclose taxation information where disclosure has been compelled.[251]

Implied abrogation of parliamentary privilege

16.195 A more controversial question is whether a secrecy provision may override parliamentary privilege by 'necessary implication'.

---

247 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.

248 Explanatory Memorandum, Auditor General Bill 1996 (Cth), [71]. See also *Migration Act 1958* (Cth) s 503A.

249 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-55.

250 Ibid sch 1 pt 1 cl 355–60(3).

251 Ibid. For more information about the intended operation of this provisions see Explanatory Material, Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth), [4.19]–[4.26].

16.196 In 1991, the Commonwealth Solicitor-General, Dr Gavan Griffith QC, provided advice on the application of secrecy provisions to officials appearing before parliamentary committees, as follows:

> Although express words are not required, a sufficiently clear intention that the provision is a declaration under section 49 [of the *Australian Constitution*] must be discernible. Accordingly, a general and almost unqualified prohibition upon disclosure is, in my view, insufficient to embrace disclosure to committees. The nature of section 49 requires something more specific.[252]

16.197 In 2000, Bret Walker SC provided advice to the NSW Legislative Council about whether a secrecy provision applied to prohibit certain witnesses from disclosing information to the budget estimates committee of the NSW Legislative Council. Walker advised that, in order for a secrecy provision to prevent the disclosure of information to a parliamentary committee, there must be either an express reference to the Houses, or that the statutory scheme would be rendered 'fatally defective' unless such an application were implied.[253]

16.198 The view that parliamentary privilege can be abrogated by 'necessary implication' has been criticised by Evans;[254] and no definitive view or court ruling has emerged.

Parliamentary processes to protect information

16.199 Where a secrecy provision does not operate to abrogate parliamentary privilege, information may be protected through other means. One such example is public interest immunity claims—that is, a claim that information should be withheld from a parliamentary committee on grounds of public interest. The *Government Guidelines for Official Witnesses Before Parliamentary Committees and Related Matters* advise that considerations that may affect a decision about whether to make documents or information available may include—in addition to whether disclosure of the information could cause harm to specified public interests—whether the information is covered by a secrecy provision.[255] Another practical way to afford some protection to sensitive information is to have this adduced in camera—that is, in a closed session.[256]

ALRC's views

16.200 Parliamentary privilege will normally override secrecy provisions, permitting the disclosure of protected information to Parliament or a parliamentary committee. This override will be supported by the exception for disclosures in the course of an

---

252 Explanatory Memorandum, Parliamentary Privileges Amendment (Effect of Other Laws) Bill 1991 (Cth).

253 J Evans, 'Orders for Papers and Executive Privilege: Committee Inquiries and Statutory Secrecy Provisions' (2002) 17(2) *Australian Parliamentary Review* 198, 210.

254 H Evans (ed), *Odgers' Australian Senate Practice* (12th ed, 2008).

255 Parliament of Australia—Senate, *Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters* (1989), [2.33].

256 Ibid, [2.35]–[2.38].

officer's duties in the recommended general secrecy offence and most specific secrecy offences. In a small number of situations, however, the disclosure of certain information to Parliament or parliamentary committees may not be the desired outcome. Here, any legislative intent to abrogate parliamentary privilege should be clearly stated in the provision and supporting documents, as for example in the Tax Laws Exposure Draft Bill.[257]

257 Exposure Draft, Tax Laws Amendment (Confidentiality of Taxpayer Information) Bill 2009 (Cth) sch 1 pt 1 cl 355-60(3).

Appendix 1. List of Submissions

Name	*Submission Number*	*Date*
Attorney-General's Department	SR 36	6 March 2009
	SR 67	14 August 2009
Australian Bureau of Statistics	SR 28	24 March 2009
	SR 58	7 August 2009
Australian Commission for Law Enforcement Integrity	SR 18	18 February 2009
	SR 84	11 September 2009
Australian Competition & Consumer Commission	SR 11	12 February 2009
Australian Crime Commission	SR 75	19 August 2009
Australian Federal Police	SR 33	3 March 2009
	SR 70	14 August 2009
Australian Human Rights Commission	SR 61	10 August 2009
Australian Intelligence Community	SR 37	6 March 2009
	SR 77	20 August 2009
Australian Press Council	SR 16	18 February 2009
	SR 62	12 August 2009
Australian Privacy Foundation	SR 71	16 August 2009

Australian Prudential Regulation Authority	SR 12	13 February 2009
	SR 52	6 August 2009
Australian Public Service Commission	SR 56	7 August 2009
Australian Securities & Investments Commission	SR 41	17 March 2009
Australian Taxation Office	SR 13	16 February 2009
	SR 55	7 August 2009
Australian Transaction Reports and Analysis Centre	SR 31	2 March 2009
	SR 73	17 August 2009
Australia's Right to Know	SR 35	6 March 2009
	SR 72	17 August 2009
A J Brown	SR 44	18 May 2009
J Butterworth	SR 07	9 February 2009
B Calcutt	SR 10	11 February 2009
A Chynoweth	SR 06	2 February 2009
Civil Liberties Australia	SR 47	27 July 2009
Clerk of the Senate	SR 03	23 January 2009
	SR 48	31 July 2009
Commonwealth Director of Public Prosecutions	SR 17	18 February 2009
	SR 65	13 August 2009
Commonwealth Ombudsman	SR 20	19 February 2009
	SR 54	7 August 2009
Community and Disability Services Ministers' Advisory Council	SR 80	28 August 2009

Community and Public Sector Union	SR 32	2 March 2009
	SR 57	7 August 2009
Confidential	SR 09	11 February 2009
Confidential	SR 21	19 February 2009
Department of Climate Change	SR 27	23 February 2009
Department of Defence	SR 69	14 August 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
	SR 68	14 August 2009
Department of Health and Ageing	SR 81	28 August 2009
Department of Human Services	SR 26	20 February 2009
	SR 83	8 September 2009
Department of Immigration and Citizenship	SR 59	7 August 2009
N Edwards	SR 08	10 February 2009
Fairness in Child Support	SR 23	19 February 2009
R Fraser	SR 42	23 March 2009
	SR 78	21 August 2009
Indigenous Business Australia	SR 64	13 August 2009
IP Australia	SR 05	4 February 2009
	SR 76	19 August 2009
Jennifer	SR 43	6 March 2009
Law Council of Australia	SR 30	27 February 2009

Liberty Victoria	SR 19	18 February 2009
	SR 50	5 August 2009
L McNamara	SR 51	6 August 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
	SR 63	12 August 2009
Non-Custodial Parents Party	SR 04	3 February 2009
	SR 82	3 September 2009
NSW Young Lawyers Human Rights Committee	SR 34	4 March 2009
Office of the Privacy Commissioner	SR 46	24 June 2009
	SR 66	13 August 2009
PricewaterhouseCoopers Australia	SR 53	7 August 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
	SR 79	24 August 2009
The Treasury	SR 22	19 February 2009
	SR 60	10 August 2009

I Turnbull	SR 15	17 February 2009
	SR 49	5 August 2009
Whistleblowers Australia	SR 40	10 March 2009
	SR 74	17 August 2009

Appendix 2. List of Agencies, Organisations and Individuals Consulted

Name	*Location*
Australian Bureau of Statistics	Sydney
Australian Electoral Commission	Canberra
Australian Federal Police	Canberra
Australian Government Attorney-General's Department	Canberra
Australian Government Information Management Office	Canberra
Australian Government Solicitor	Canberra
Australian Intelligence Community	Canberra
Australian Public Service Commission	Canberra
Australian Taxation Office	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
Crime and Misconduct Commission Queensland	Brisbane
Department of Defence	Canberra
Department of Education, Employment and Workplace Relations	Canberra
Department of Families, Community Services and Indigenous Affairs	Canberra
Department of Finance and Deregulation	Canberra
Department of Human Services	Canberra
Department of the Prime Minister and Cabinet	Canberra

Mr C Erskine SC	Sydney
Government 2.0 Taskforce	Sydney
Indigenous Business Australia	Canberra
Monash University academics	Melbourne
Members of the New South Wales Bar Association	Sydney
Office of Parliamentary Counsel	Canberra
Office of the Privacy Commissioner	Sydney
Justice H Penfold, Supreme Court of the ACT	Canberra
Justice R Refshauge, Supreme Court of the ACT	Canberra
Dr D Solomon	Sydney
The Treasury	Canberra

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
ACMA	Australian Communications and Media Authority
ACS	Australian Customs Service
ACSI 33	*Australian Government Information and Communications Technology Security Manual*
ADF	Australian Defence Force
AFP	Australian Federal Police
AFP Act	*Australian Federal Police Act 1979* (Cth)
AGD	Australian Government Attorney-General's Department
AGS	Australian Government Solicitor
AIC	Australian Intelligence Community
ALRC	Australian Law Reform Commission
ALRC 77	Australian Law Reform Commission, *Open Government: A Review of the Freedom of Information Act 1982* (1995)
ALRC 85	Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983* (1998)

ALRC 95	Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia* (2002)
ALRC 98	Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (2004)
ALRC 102	Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law* (2005)
ALRC 108	Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (2008)
AMC	Australian Military Court
AML/CTF Act	*Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)
ANAO	Australian National Audit Office
APRA	Australian Prudential Regulation Authority
APRA Act	*Australian Prudential Regulation Authority Act 1998* (Cth)
APSC	Australian Public Service Commission
APS	Australian Public Service
ARC	Administrative Review Council
ARTK	Australia's Right to Know
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
ASIS	Australian Secret Intelligence Service
ATO	Australian Taxation Office
ATSI Act	*Aboriginal and Torres Strait Islander Act 2005* (Cth)

AUSTRAC	Australian Transaction Reports and Analysis Centre
CAC Act	*Commonwealth Authorities and Companies Act 1997* (Cth)
CDPP	Commonwealth Director of Public Prosecutions
CLA	Civil Liberties Australia
CMC	Crime and Misconduct Commission Queensland
CPSU	Community and Public Sector Union
CRS	Commonwealth Rehabilitation Service
DAF	Deny Access Facility
DEEWR	Department of Education, Employment and Workplace Relations
DFAT	Department of Foreign Affairs and Trade
DFD Act	*Defence Force Discipline Act 1982* (Cth)
DFO	Defence Force Ombudsman
DHS	Department of Human Services
DIAC	Department of Immigration and Citizenship
DIO	Defence Intelligence Organisation
DoHA	Department of Health and Ageing
DP 74	Australian Law Reform Commission, *Review of Secrecy Laws*, Discussion Paper 74 (2009)
FaHCSIA	Department of Families, Housing, Community Services and Indigenous Affairs

FMA Act	*Financial Management and Accountability Act 1997* (Cth)
FMG 3	*Financial Management Guidance No 3—Guidance on Confidentiality in Procurement*
FOI	Freedom of information
FOI Act	*Freedom of Information Act 1982* (Cth)
IBA	Indigenous Business Australia
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
IP 34	Australian Law Reform Commission *Review of Secrecy Laws*, Issues Paper 34 (2008)
IPPs	Information Privacy Principles
MOPS Act	*Members of Parliament (Staff) Act 1984* (Cth)
MOU	Memorandum of understanding
MPC	Merit Protection Commissioner
NCIDD	National Criminal Investigation DNA Database
NPPs	National Privacy Principles
ONA	Office of National Assessments
PBAC	Pharmaceutical Benefits Advisory Committee
PBS	Pharmaceutical Benefits Scheme
PIA	Privacy Impact Assessment
PIAC	Public Interest Advocacy Centre
PSM	*Australian Government Protective Security Manual*

SES	Senior Executive Service
SSAT	Social Security Appeals Tribunal

Appendix 4. Table of Secrecy Provisions

As part of the background research for this Inquiry, the ALRC undertook a 'mapping exercise' to identify and analyse secrecy provisions in Commonwealth legislation. The definition of 'secrecy provision' is discussed in Chapter 1. The ALRC identified 506 provisions, which are set out in the following table.

The first section of the table lists the provisions in Commonwealth legislation that expressly impose criminal sanctions for breach of secrecy or confidentiality obligations. The second section lists all other provisions that impose such obligations but do not expressly impose criminal sanctions. Some of these provisions create a 'duty not to disclose' that may attract criminal sanctions under s 70 of the *Crimes Act 1914* (Cth). Where, in the ALRC's view, the language of a provision may indicate an intention to enliven the criminal offence in s 70, such provisions have been marked with an asterisk. Provisions that only set out exceptions to secrecy or confidentiality obligations and other associated matters are not included.

Criminal secrecy offences

Legislation	Provision	Administrative Arrangements Order
A New Tax System (Australian Business Number) Act 1999	s 30	The Treasury
A New Tax System (Bonuses for Older Australians) Act 1999	s 55	The Treasury
A New Tax System (Family Assistance)(Administration) Act 1999	ss 164; 165; 166(1), (2); 163	Families, Housing, Community Services and Indigenous Affairs
A New Tax System (Goods and Services Tax Administration) Act 1999	s 68	The Treasury
Aboriginal and Torres Strait Islander Act 2005	ss 191; 193S; 200A	Families, Housing, Community Services and Indigenous Affairs

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Aboriginal Land Rights (Northern Territory) Act 1976	s 23E(2), (4)	Families, Housing, Community Services and Indigenous Affairs
Age Discrimination Act 2004	s 60	Attorney-General
Aged Care Act 1997	ss 86-2; 86-5; 86-6; 86-7	Health and Ageing
Agricultural and Veterinary Chemicals Code Act 1994	s 162(1), (8), (9)	Agriculture, Fisheries and Forestry
Agricultural and Veterinary Chemicals Code Regulations 1995	reg 69	Agriculture, Fisheries and Forestry
Anti-Money Laundering and Counter-Terrorism Financing Act 2006	ss 121; 122; 123; 127; 128(5), (10); 130; 131(4)	Attorney-General
Auditor-General Act 1997	s 36(1), (2B), (3)	Prime Minister and Cabinet
AusCheck Act 2007	s 15	Attorney-General
Australian Citizenship Act 2007	ss 42; 43	Immigration and Citizenship
Australian Crime Commission Act 2002	ss 25A(9); 29B(1), (3); 51	Attorney-General
Australian Federal Police Act 1979	ss 40ZA; 60A	Attorney-General
Australian Hearing Services Act 1991	s 67(8)	Health and Ageing
Australian Human Rights Commission Act 1986	s 49	Attorney-General
Australian Institute of Health and Welfare Act 1987	s 29	Health and Ageing

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Australian Postal Corporation Act 1989	ss 90H; 90LB; 90LE	Broadband, Communications and the Digital Economy
Australian Prudential Regulation Authority Act 1998	s 56	The Treasury
Australian Securities and Investments Commission Act 2001	s 127(4EA), (4F)	The Treasury
Australian Security Intelligence Organisation Act 1979	ss 18; 34ZS(1), (2); 81; 92(1), (1A)	Attorney-General
Australian Sports Anti-Doping Authority Act 2006	ss 71; 72	Health and Ageing
Australian Trade Commission Act 1985	s 94	Foreign Affairs and Trade
Aviation Transport Security Act 2004	s 74	Infrastructure, Transport, Regional Development and Local Government
Aviation Transport Security Regulations 2005	regs 2.06; 4.46(2), (3), (4)	Infrastructure, Transport, Regional Development and Local Government
Banking Act 1959	ss 11CF; 52E	The Treasury
Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992	s 25	Broadband, Communications and the Digital Economy
Building and Construction Industry Improvement Act 2005	s 65	Education, Employment and Workplace Relations
Census and Statistics Act 1905	s 19	The Treasury

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Chemical Weapons (Prohibition) Act 1994	s 102(2), (3A), (3C)	Foreign Affairs and Trade
Child Care Act 1972	ss 12K; 12L; 12Q; 12R; 12S	Education, Employment and Workplace Relations
Child Support (Assessment) Act 1989	ss 150; 150AA	Families, Housing, Community Services and Indigenous Affairs
Child Support (Registration and Collection) Act 1988	ss 16; 16AA; 58	Families, Housing, Community Services and Indigenous Affairs
Civil Aviation Act 1988	s 32AP(1), (2)	Infrastructure, Transport, Regional Development and Local Government
Civil Aviation Regulations 1988	reg 132	Infrastructure, Transport, Regional Development and Local Government
Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992	s 14	Education, Employment and Workplace Relations
Commonwealth Electoral Act 1918	ss 91A; 91B(2), (3); 189B(1), (2), (3); 323	Finance and Deregulation
Commonwealth Functions (Statutes Review) Act 1981	s 234	The Treasury
Competition Policy Reform (Transitional Provisions) Regulations 1995	reg 6	The Treasury

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Comprehensive Nuclear Test-Ban Treaty Act 1998	s 74(2), (4)	Foreign Affairs and Trade
Copyright Act 1968	s 203E	Attorney-General
Corporations (Aboriginal and Torres Strait Islander) Act 2006	ss 175-10; 183-1; 472-1; 604-15; 604-20	Families, Housing, Community Services and Indigenous Affairs
Crimes Act 1914	ss 3ZQJ; 3ZQT; 15XS(1), (2); 23XG; 23YO; 70(1), (2); 79(2), (3), (4), (5), (6); 83	Attorney-General
Criminal Code	ss 91.1(1), (2), (3), (4); 105.41(1), (2), (3), (4A), (5), (6), (7)	Attorney-General
Crimes (Taxation Offences) Act 1980	s 4(1), (1A), (1AA), (4), (5)	The Treasury
Customs Act 1901	s 64ADA	Attorney-General
Customs Administration Act 1985	s 16	Attorney-General
Dairy Produce Act 1986	s 119(2)(a), (b); sch 2 cl 43	Agriculture, Fisheries and Forestry
Data-matching Program (Assistance and Tax) Act 1990	s 15	Families, Housing, Community Services and Indigenous Affairs
Defence (Inquiry) Regulations 1985	reg 63	Defence
Defence (Special Undertakings) Act 1952	s 9	Defence
Defence Act 1903	s 73A	Defence
Defence Force Discipline Act 1982	ss 16; 58	Defence

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Dental Benefits Act 2008	ss 34; 43; 44; 45; 46	Health and Ageing
Designs Act 2003	s 109	Innovation, Industry, Science and Research
Development Allowance Authority Act 1992	s 114	The Treasury
Disability Discrimination Act 1992	s 127	Attorney-General
Disability Services Act 1986	s 28	Families, Housing, Community Services and Indigenous Affairs
Environment Protection (Alligator Rivers Region) Act 1978	s 31(2), (4)	Environment, Water, Heritage and the Arts
Environment Protection and Biodiversity Conservation Act 1999	sch 1 cll 51, 53	Environment, Water, Heritage and the Arts
Epidemiological Studies (Confidentiality) Act 1981	ss 4; 6	Health and Ageing
Equal Opportunity for Women in the Workplace Act 1999	s 32	Families, Housing, Community Services and Indigenous Affairs
Excise Act 1901	s 159	The Treasury
Export Finance and Insurance Corporation Act 1991	s 87(5)	Foreign Affairs and Trade
Financial Transaction Reports Act 1988	s 16(5A), (5AA)	Attorney-General
First Home Saver Accounts Act 2008	s 70	The Treasury
Fisheries Management Act 1991	sch 1A cl 53	Agriculture, Fisheries and Forestry

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Food Standards Australia New Zealand Act 1991	s 114(8)	Health and Ageing
Fringe Benefits Tax Assessment Act 1986	s 5	The Treasury
Gene Technology Act 2000	s 187(1), (2)	Health and Ageing
Health Insurance Act 1973	ss 124Y; 130(1), (3B), (3C), (4), (9), (14), (15), (17), (19), (21), (22)	Health and Ageing
Higher Education Funding Act 1988	s 78(4)	Education, Employment and Workplace Relations
Higher Education Support Act 2003	ss 179-10; 179-35	Education, Employment and Workplace Relations
Income Tax Assessment Act 1936	ss 16; 16A	The Treasury
Income Tax Assessment Act 1997	s 396-95	The Treasury
Inspector of Transport Security Act 2006	ss 35(7); 36(7); 37(8); 49(2); 56; 60(5); 63(4), (5); 67; 75	Infrastructure, Transport, Regional Development and Local Government
Inspector-General of Intelligence and Security Act 1986	s 34	Prime Minister and Cabinet
Inspector-General of Taxation Act 2003	s 37	The Treasury
Insurance Act 1973	s 107	The Treasury
Intelligence Services Act 2001	ss 39; 39A; 40; 41; sch 1 cl 9	Defence

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
International Criminal Court Act 2002	s 92	Attorney-General
Law Enforcement Integrity Commissioner Act 2006	ss 90; 92(1), (3), (5); 207	Attorney-General
Life Insurance Act 1995	ss 156E; 230E	The Treasury
Maritime Transport and Offshore Facilities Security Act 2003	s 40	Infrastructure, Transport, Regional Development and Local Government
Medical Indemnity Act 2002	s 77	Health and Ageing
Migration Act 1958	ss 261AKD; 336C; 336E; 377; 439	Immigration and Citizenship
Mutual Assistance in Criminal Matters Act 1987	ss 34V; 43B; 43C	Attorney-General
National Blood Authority Act 2003	s 11	Health and Ageing
National Environment Protection Measures (Implementation) Act 1998	s 36	Environment, Water, Heritage and the Arts
National Greenhouse and Energy Reporting Act 2007	s 23	Climate Change (Part of the Prime Minister and Cabinet Portfolio)
National Health Act 1953	ss 135A(1), (4), (9), (13), (14), (16), (18), (20), (21); 135AAA(1), (3), (6), (8)	Health and Ageing
National Health and Medical Research Council Act 1992	s 80(2), (7), (11)	Health and Ageing
National Health Security Act 2007	ss 21, 90	Health and Ageing
National Measurement Act 1960	s 19H	Innovation, Industry, Science and Research

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
National Residue Survey Administration Act 1992	s 11(5)	Agriculture, Fisheries and Forestry
National Water Commission Act 2004	s 43	Environment, Water, Heritage and the Arts
Nuclear Non-Proliferation (Safeguards) Act 1987	s 71	Foreign Affairs and Trade
Offshore Minerals Act 1994	s 374(1), (2)	Resources, Energy and Tourism
Offshore Petroleum and Greenhouse Gas Storage Act 2006	s 758(1), (3)	Resources, Energy and Tourism
Ombudsman Act 1976	s 35(2), (5)	Prime Minister and Cabinet
Parliamentary Commission of Inquiry (Repeal) Act 1986	s 7	Prime Minister and Cabinet
Parliamentary Privileges Act 1987	s 13	Attorney-General
Patents Act 1990	ss 152(4); 173; 184	Innovation, Industry, Science and Research
Petroleum Resource Rent Tax Assessment Act 1987	ss 17; 18	The Treasury
Pooled Development Funds Act 1992	s 71	Innovation, Industry, Science and Research
Port Statistics Act 1977	s 7	Infrastructure, Transport, Regional Development and Local Government

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Postal and Telecommunications Commissions (Transitional Provisions) Act 1975	s 37	Broadband, Communications and the Digital Economy
Privacy Act 1988	ss 80Q; 96	Prime Minister and Cabinet
Private Health Insurance Act 2007	ss 323-1; 323-40; 323-45; 323-50; 323-55	Health and Ageing
Proceeds of Crime Act 1987	s 74(1), (2)	Attorney-General
Proceeds of Crime Act 2002	ss 210(1), (2); 217; 223(1), (2), (3)	Attorney-General
Product Grants and Benefits Administration Act 2000	s 47	The Treasury
Productivity Commission Act 1998	s 53	The Treasury
Public Service Regulations 1999	reg 7.6	Prime Minister and Cabinet
Racial Discrimination Act 1975	s 27F(1)	Attorney-General
Referendum (Machinery Provisions) Act 1984	s 116	Finance and Deregulation
Renewable Energy (Electricity) Act 2000	s 127	Climate Change (Part of the Prime Minister and Cabinet Portfolio)
Research Involving Human Embryos Act 2002	s 30(1), (2)	Health and Ageing
Reserve Bank Act 1959	ss 79A; 79B	The Treasury
Sex Discrimination Act 1984	ss 92; 112	Attorney-General
Social Security (Administration) Act 1999	ss 203; 204; 205; 206	Families, Housing, Community Services and Indigenous Affairs

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Social Welfare Commission (Repeal) Act 1976	s 8	Families, Housing, Community Services and Indigenous Affairs
Space Activities Act 1998	s 96	Innovation, Industry, Science and Research
Student Assistance Act 1973	ss 12ZU; 352; 353; 357; 358; 359	Education, Employment and Workplace Relations
Superannuation Contributions Tax (Assessment and Collection) Act 1997	s 32	The Treasury
Superannuation Contributions Tax (Members of Constitutionally Protected Superannuation Funds) Assessment and Collection Act 1997	s 28	The Treasury
Superannuation (Government Co-contribution for Low Income Earners) Act 2003	s 53	The Treasury
Superannuation Guarantee (Administration) Act 1992	s 45	The Treasury
Superannuation Industry (Supervision) Act 1993	s 252C	The Treasury
Superannuation (Resolution of Complaints) Act 1993	s 63(2), (3B)	The Treasury
Superannuation (Unclaimed Money and Lost Members) Act 1999	s 32	The Treasury
Surveillance Devices Act 2004	s 45(1), (2)	Attorney-General
Tax Agent Services Act 2009	s 70-35	The Treasury

Criminal secrecy offences		
Legislation	**Provision**	**Administrative Arrangements Order**
Taxation Administration Act 1953	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	The Treasury
Taxation (Interest on Overpayments and Early Payments) Act 1983	s 8	The Treasury
Telecommunications (Interception and Access) Act 1979	ss 63(1), (2); 133; 182	Attorney-General
Termination Payments Tax (Assessment and Collection) Act 1997	s 23	The Treasury
Torres Strait Fisheries Act 1984	sch 2 cll 51; 53	Agriculture, Fisheries and Forestry
Torres Strait Fisheries Regulations 1985	reg 13	Agriculture, Fisheries and Forestry
Trade Practices Act 1974	ss 95ZP; 95ZQ; sch s 10.89	The Treasury
Transport Safety Investigation Act 2003	ss 26(2)(a), (b); 53(1), (2); 60(1), (2), (3)	Infrastructure, Transport, Regional Development and Local Government
Wheat Export Marketing Act 2008	s 74	Agriculture, Fisheries and Forestry
Witness Protection Act 1994	s 22(1), (2)	Attorney-General
Wheat Export Marketing (Repeal and Consequential Amendments) Act 2008	sch 3 item 6	Agriculture, Fisheries and Forestry

Other secrecy provisions		
Legislation	**Provision**	**Administrative Arrangements Order**
A New Tax System (Australian Business Number) Act 1999	s 26	The Treasury
Aged Care Act 1997	ss 62-1; 63-1AA	Health and Ageing
Air Navigation (Confidential Reporting) Regulations 2006	reg 14	Infrastructure, Transport, Regional Development and Local Government
Air Navigation Regulations 1947	reg 12	Infrastructure, Transport, Regional Development and Local Government
Airports (Building Control) Regulations 1996	reg 4.03*	Infrastructure, Transport, Regional Development and Local Government
Airports (Environment Protection) Regulations 1997	reg 10.06*	Infrastructure, Transport, Regional Development and Local Government
Archives Act 1983	s 30A*	Prime Minister and Cabinet
Auditor-General Act 1997	s 37	Prime Minister and Cabinet
Australian Crime Commission Act 2002	ss 9; 59; 60(5); 61	Attorney-General
Australian Federal Police Regulations 1979	regs 12; 13B*; 13C	Attorney-General
Australian Hearing Services Act 1991	s 67(1)*	Health and Ageing

Other secrecy provisions		
Legislation	**Provision**	**Administrative Arrangements Order**
Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989	s 41	Innovation, Industry, Science and Research
Australian Organ and Tissue Donation and Transplantation Authority Act 2008	s 58	Health and Ageing
Australian Securities and Investments Commission Act 2001	ss 127(1); 213; 237	The Treasury
Australian Wine and Brandy Corporation (Annual General Meeting of the Industry) Regulations 1999	reg 9	Agriculture, Fisheries and Forestry
Bankruptcy Regulations 1996	regs 8.05O; 8.32	Attorney-General
Building and Construction Industry Improvement Act 2005	s 66	Education, Employment and Workplace Relations
Cadet Forces Regulations 1977	sch 4 cl 5	Defence
Census and Statistics Act 1905	ss 12; 13; 19A	The Treasury
Commonwealth Electoral Act 1918	s 90B	Finance and Deregulation
Crimes Act 1914	s 23XWO	Attorney-General
Designs Act 2003	ss 61; 108	Innovation, Industry, Science and Research
Environment Protection and Biodiversity Conservation Act 1999	ss 131AA(4); 133(4); 143(6); 146B(4); 170B; 189B*; 251(3)*; 324R*; 341R*; 390R*	Environment, Water, Heritage and the Arts

Other secrecy provisions		
Legislation	**Provision**	**Administrative Arrangements Order**
Export Finance and Insurance Corporation Act 1991	s 87(4)*	Foreign Affairs and Trade
Family Law Act 1975	ss 10D; 10H	Attorney-General
Film Licensed Investment Company (Application) Rules 2005	r 17*	Environment, Water, Heritage and the Arts
Fisheries Administration Act 1991	s 101(6)	Agriculture, Fisheries and Forestry
Food Standards Australia New Zealand Act 1991	s 114*	Health and Ageing
Health Insurance Regulations 1975	reg 23C(2)(a)	Health and Ageing
Industry Research and Development Act 1986	s 47	Innovation, Industry, Science and Research
Inspector of Transport Security Act 2006	ss 37(7); 61; 62; 63(1), (2), (3); 64(2), (3), (4), (5); 68; 69; 77(9)	Infrastructure, Transport, Regional Development and Local Government
International Criminal Court Act 2002	s 13*	Attorney-General
Migration Act 1958	ss 46A(5); 46B(5); 48B(4); 72(5); 91F(4); 91L(4); 91Q; 91Y; 195A(7); 197AG(2); 503A(1)*, (5)	Immigration and Citizenship
Military Rehabilitation and Compensation Act 2004	s 409*	Veterans' Affairs
National Health and Medical Research Council Act 1992	s 78(1)*	Health and Ageing
National Health Regulations 1954	reg 32*	Health and Ageing

Other secrecy provisions

Legislation	Provision	Administrative Arrangements Order
National Residue Survey Administration Act 1992	s 11(1)	Agriculture, Fisheries and Forestry
National Workplace Relations Consultative Council Act 2002	s 5	Education, Employment and Workplace Relations
Native Title Act 1993	ss 24BF(2); 24CF(2); 24CI(3); 24DG(2); 24DJ(3); 31(4); 44B(4A); 44F(2); 86F(2A); 98A(2); 203BK(4)	Attorney-General
Occupational Health and Safety (Safety Standards) Regulations 1994	regs 8.61; 9.68	Education, Employment and Workplace Relations
Offshore Petroleum and Greenhouse Gas Storage Act 2006	ss 712; 713; 715; 716; 766; sch 5 cl 4	Resources, Energy and Tourism
Ombudsman Act 1976	ss 19U; 35A; 35B; 35C	Prime Minister and Cabinet
Parliamentary Service Act 1999	s 13(6)	Prime Minister and Cabinet
Patents Act 1990	ss 56; 183*	Innovation, Industry, Science and Research
Privacy (Private Sector) Regulations 2001	sch 1 cl 4.6	Prime Minister and Cabinet
Public Service Act 1999	s 13(6)	Prime Minister and Cabinet
Public Service Regulations 1999	regs 2.1*; 6.3	Prime Minister and Cabinet
Research Involving Human Embryos Act 2002	s 29(4)	Health and Ageing

Other secrecy provisions		
Legislation	**Provision**	**Administrative Arrangements Order**
Social Security (Administration) Act 1999	sch 3 cl 19	Families, Housing, Community Services and Indigenous Affairs
Telecommunications (Consumer Protection and Service Standards) Act 1999	ss 22; 22A	Broadband, Communications and the Digital Economy
Telecommunications (Interception and Access) Act 1979	s 202	Attorney-General
Therapeutic Goods Act 1989	s 9C	Health and Ageing
Trade Marks Act 1995	s 258	Innovation, Industry, Science and Research
Trade Practices Act 1974	sch ss 10.37; 10.88	Infrastructure, Transport, Regional Development and Local Government
Trade Practices Act 1974	ss 44AAF; 89(5A); 95; 95AI; 95AZA; 95ZN; 155AA*; 155AAA*	The Treasury
Trade Practices Regulations 1974	reg 7D	The Treasury
Veterans' Entitlements Act 1986	ss 34; 35H; 36L; 37L; 38L; 45Q; 57E; 79I; 93ZE; 116D; 118ZF; 118ZX; 137; 140; 196ZD	Veterans' Affairs
Water Act 2007	s 215	Environment, Water, Heritage and the Arts
Witness Protection Act 1994	s 16*	Attorney-General

Appendix 5. Extracts of Key Secrecy Provisions

Contents

The full text of a number of the principal provisions referred to in this Report are set out below.

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).

Criminal Code Act 1995 (Cth)

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 (other than an official of a registered industrial organisation) 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

(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

(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.

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.