Australian Government
Australian Law Reform Commission

Review of Secrecy Laws

ISSUES PAPER

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

ISSUES PAPER 34
December 2008

This Issues Paper reflects the law as at 1 November 2008.

ISBN-978-0-9804153-4-6

Commission Reference: IP 34

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

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

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

E-mail: info@alrc.gov.au

ALRC homepage: www.alrc.gov.au

Printed by Ligare

Making a submission

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

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

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

Open inquiry policy

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

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

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

Submissions should be sent to:

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

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

<www.alrc.gov.au>

The closing date for submissions in response to IP 34 is 19 February 2009.

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

Senior Legal Officers

Carolyn Adams
Bruce Alston
Kate Connors
Isabella Cosenza

Legal Officers

Lisa Eckstein
Althea Gibson
Erin Mackay

Research Manager

Jonathan Dobinson

Librarian

Carolyn Kearney

Project Assistants

Tina O'Brien

Legal Interns

Larisa Michalko
Tracy Nau
Katie Schafer
Smriti Sriram
Rebecca Zaman

Advisory Committee Members

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

List of Questions

1. Introduction to the Inquiry

1–1 In light of freedom of information laws and other modern moves towards greater openness and accountability on the one hand, and the current international security environment on the other, are secrecy laws still relevant and necessary? Is a statutory duty on Commonwealth officers not to disclose information necessary or desirable? Are general law obligations sufficient and appropriate ways by which the disclosure of Commonwealth information may be regulated?

1–2 Do federal secrecy provisions inhibit unduly the sharing of information within and between law enforcement agencies, governments, and between governments and the private sector?

2. Overview of Secrecy Provisions in Commonwealth Legislation

2–1 Should the unauthorised handling of Commonwealth information remain subject to a general criminal offence? If so, should s 70 of the *Crimes Act 1914* (Cth) be repealed and replaced by an updated offence in the *Criminal Code* (Cth)?

2–2 If it is appropriate to retain a general criminal offence for unauthorised handling of Commonwealth information, how should that provision be framed? Is it appropriate for such a provision to rely on a duty arising separately under the general law or under other legislative provisions?

2–3 Given the overlap between s 70 of the *Crimes Act 1914* (Cth), s 79 of the *Crimes Act* and s 91.1 of the *Criminal Code* (Cth), should any of the offences currently in s 79 be retained and replaced by updated offences in the *Criminal Code*? If so, how should those offences be framed?

2–4 Given that the consolidation of secrecy laws is being considered in relation to taxation secrecy and disclosure provisions, in what other legislative areas, if any, is this appropriate?

2–5 Should Commonwealth secrecy provisions aim to protect:

(a) specific types of information? If so, what types of information should be protected by the provisions?

(b) information held by certain persons or agencies? If so, which persons or agencies should be regulated by the provisions?

(c) information, the disclosure of which may harm a specified public interest? If so, what public interest or interests should be protected by the provisions?

2–6 Should secrecy provisions establish a general prohibition on disclosure of certain information and then attempt to codify the circumstances in which disclosure is allowed?

2–7 Should secrecy provisions be consolidated, wherever possible, into a single provision in each Act or regulation?

2–8 Are there any other issues in relation to the form of secrecy provisions that the ALRC should consider in the course of this Inquiry?

3. Secrecy Provision Elements

3–1 In what circumstances should secrecy provisions regulate the behaviour of persons other than Commonwealth officers such as: consultants and others who provide goods and services to the Australian Government; those who enter into arrangements with the Australian Government; and state and territory government employees?

3–2 Some secrecy provisions—for example a number of provisions relating to defence and security—regulate the activities of anyone who comes into possession or control of documents or information. When should secrecy provisions regulate the behaviour of 'any person', including members of the media?

3–3 In what circumstances should secrecy provisions regulate those who have been Commonwealth officers, or who have held other positions subject to Commonwealth secrecy provisions, but who are no longer in those positions?

3–4 Should secrecy provisions regulate only the disclosure of information or is it appropriate to regulate other conduct such as the unauthorised receipt, collection, use or recording of information?

3–5 Should all secrecy provisions seek to regulate both initial and subsequent unauthorised handling of Commonwealth information?

3–6 In what circumstances might it be appropriate to have fault elements other than intent and recklessness in secrecy provisions?

3–7 Should all secrecy provisions expressly require that the unauthorised conduct cause, be likely to cause, or be intended to cause harm to a specified public interest?

3–8 Does reg 2.1 of the *Public Service Regulations 1999* (Cth) provide an appropriate model for protecting Commonwealth information in a way that is consistent with the implied constitutional guarantee of freedom of political communication?

3–9 Are there other secrecy provisions that may be inconsistent with the implied constitutional guarantee of freedom of political communication?

4. Exceptions and Defences

4–1 If it is appropriate to retain a general criminal offence for unauthorised handling of Commonwealth information, what exceptions or defences should be incorporated in such a provision? For example, should such an offence apply only where the person concerned had reasonable cause to believe that his or her conduct would harm specified public interests? If so, should such a provision be framed as an exception or as a defence?

4–2 In what circumstances should Commonwealth secrecy laws permit the disclosure of Commonwealth information:

(a) in the performance of a Commonwealth officer's functions and duties;

(b) as required or authorised by legislation;

(c) on the authority of specified persons;

(d) to ministers or other specified persons or entities;

(e) for the purposes of legal proceedings or law enforcement; or

(f) for other purposes?

4–3 When should provisions in Commonwealth secrecy laws permitting the handling of information generally be framed as exceptions or defences?

4–4 When should Commonwealth secrecy laws include an exception or defence permitting disclosure of personal information, for example, with the consent of the person to whom the information relates or where the personal information is already in the public domain?

4–5 Should the exceptions and defences incorporated in Commonwealth secrecy laws be reviewed to ensure compliance with current drafting guidelines, such as those issued by the Attorney-General's Department and the Office of Parliamentary Counsel?

4–6 What should be the relationship between exceptions and defences provided under Commonwealth secrecy laws and possible new Commonwealth public interest disclosure legislation? For example, should public interest disclosure be incorporated as an exception to criminal offences for unauthorised handling of Commonwealth information?

4–7 Should new public interest disclosure legislation, if enacted, exclude disclosure by Commonwealth officers employed by certain agencies—such as those involved in protecting national security?

4–8 Are there other issues in relation to exceptions and defences in Commonwealth secrecy laws that the ALRC should consider in the course of this Inquiry?

5. Penalties

5–1 When should unauthorised handling of Commonwealth information be subject to criminal penalties? Which factors should determine whether or not it is appropriate for criminal penalties to apply?

5–2 In what circumstances, if any, is it appropriate for secrecy provisions to specify:

(a) fines for individuals and corporations different from those that would apply if the formulas set out in the *Crimes Act 1914* (Cth) were adopted?

(b) penalties different to those that would apply if the alternate penalties for proceeding summarily on an indictable offence set out in the *Crimes Act* were adopted?

5–3 In what circumstances, if any, is it appropriate for a secrecy provision to specify a penalty punishable on summary conviction when, under the *Crimes Act 1914* (Cth), an offence carrying that maximum penalty would otherwise be tried before a jury on indictment?

5–4 What is the best way to achieve consistency in the maximum criminal penalties for breach of secrecy provisions? Should maximum penalties be referable to the type of information protected, conduct proscribed, fault element; whether or not the conduct harmed the public interest; or a combination of these factors?

5–5 If secrecy provisions apply, or are to apply, to both initial and subsequent unauthorised handling of Commonwealth information, should the maximum penalties for initial and subsequent unauthorised handling be consistent?

5–6 Should there be benchmarks for the maximum levels of criminal penalties that apply to secrecy offences according to their categorisation? If so, what should those benchmarks be? For example, should the maximum level of penalty that attaches to offences involving:

(a) the unauthorised handling of national security information; or

(b) an element of likelihood of harm to the public interest

carry higher maximum criminal penalties than those that do not?

5–7 Are there any circumstances in which it is appropriate for a secrecy provision to give a sentencing court complete discretion as to the maximum level of penalty that is to apply (as is the case in the secrecy provision in the *Defence Act 1903* (Cth))?

5–8 Given conflicting drafting guidelines about what level of fine amounts to a significant criminal penalty—which should therefore only attach to offences in primary legislation—what is an appropriate maximum level of fine for a secrecy offence that is located in a regulation?

5–9 Should those secrecy offence provisions that are currently located in regulations and which either:

(a) carry a term of imprisonment or a significant fine; or

(b) specify a duty of non-disclosure which attracts a term of imprisonment because of the application of s 70 of the *Crimes Act 1914* (Cth)

be relocated to primary legislation?

5–10 Should all secrecy provisions be drafted to ensure that the consequences of breach are clear on their face? For example, if the penalty for breaching a duty of non-disclosure set out in a secrecy provision is set out in another legislative provision (such as s 70 of the *Crimes Act 1914* (Cth)) should the secrecy provision cross-refer expressly to the other legislative provision?

5–11 Is there a need to redraft those secrecy offence provisions that refer to maximum fines in monetary terms rather than penalty units or is this unnecessary because of the application of s 4AB of the *Crimes Act 1914* (Cth)?

5–12 Are the range and level of administrative penalties available for breaches of secrecy provisions committed by Commonwealth officers—for example, the current maximum deduction of 2% of an Australian Public Service employee's annual salary—adequate and appropriate?

5–13 Are there any breaches of secrecy provisions which should only give rise to administrative penalties?

5–14 In circumstances where administrative penalties are unavailable to address breaches of secrecy provisions—namely where such breaches are committed by private sector employees or former Commonwealth officers—are there other ways of addressing this gap in application?

5–15 In practice, are administrative penalties for breach of similar types of secrecy provisions applied consistently across Australian Government agencies? If not, how can this inconsistency best be addressed?

5–16 Do infringement notice schemes have any role to play in offering alternative processes and penalties for enforcing and punishing breach of Commonwealth secrecy offences? If so, what features should such schemes have?

5–17 Is there a greater role for civil penalties to apply for unauthorised handling of Commonwealth information? If so, what model should apply?

6. Practical Framework for Protecting Commonwealth Information

6–1 Are agency policies on information handling consistent with Commonwealth secrecy laws? For example, do agency policies on information handling require a higher level of secrecy than is needed to meet obligations under Commonwealth secrecy laws?

6–2 What role do oaths or declarations of secrecy play in protecting Commonwealth information? Should they be retained?

6–3 How effective are strategies used by Australian Government agencies such as:

(a) memorandums of understanding;

(b) training and development programs; and

(c) information and communication technology systems,

in protecting Commonwealth information? Are there any other strategies for protecting Commonwealth information that the ALRC should consider?

6–4 Should secrecy laws expressly provide for injunctions to restrain unauthorised handling of Commonwealth information? If so, should this apply only to certain types of Commonwealth information, for example, national security or other sensitive Commonwealth information?

6–5 In practice, how effective are the processes set out in the *Public Service Act 1999* (Cth) and related instruments for investigating and enforcing suspected breaches of secrecy provisions that amount to breaches of the Code of Conduct?

6–6 In practice, how effective are the processes for investigating and enforcing breaches of secrecy laws by Commonwealth officers other than Australian Public Service (APS) employees? In particular, should the legislation under which these officers are employed:

(a) require that the processes for dealing with suspected misconduct that apply to APS employees be adopted, to the extent that these processes are consistent with the performance of the functions of the employing agency; and

(b) include a process for merits review of any penalties imposed?

6–7 Is there sufficient transparency in decisions to investigate breaches of secrecy provisions, for example through the *Case Categorisation and Prioritisation Model*?

6–8 Should the Attorney-General's consent be required for the commencement of prosecutions under:

(a) ss 79 or 83 of the *Crimes Act 1914* (Cth) or s 91.1 of the *Criminal Code* (Cth);

(b) secrecy provisions relating to national security and other sensitive Commonwealth information; or

(c) any other secrecy provisions?

6–9 Is there a need for any safeguards to apply where secrecy provisions could give rise to both administrative and criminal proceedings; for example, should the legislation provide for a stay of administrative proceedings to accommodate current or future criminal actions?

6–10 In practice, how effective are the mechanisms in place for monitoring and overseeing the application and enforcement of secrecy laws by Commonwealth agencies?

6–11 Are there any other issues relating to the practical framework for protecting Commonwealth information that the ALRC should consider?

7. Comparisons and Interactions with Other Laws

7–1 Given that the *Freedom of Information Act 1982* (Cth) promotes open and accountable government, and secrecy provisions protect Commonwealth information, what should be the relationship between these two regimes?

7–2 If the relationship between secrecy provisions and the *Freedom of Information Act 1982* (Cth) (FOI Act) does not strike the right balance, how should this be addressed? For example:

(a) should it be clarified that disclosure in accordance with the objects of the FOI Act overrides a secrecy provision that does not fall within the current exemptions in the Act?

(b) should the secrecy exemption in the FOI Act be amended or repealed?

7–3 Are there other aspects of the relationship between secrecy provisions and the *Freedom of Information Act 1982* (Cth) that need to be clarified?

7–4 Does the relationship between secrecy provisions and the *Privacy Act 1988* (Cth) need to be clarified? In particular, should secrecy provisions regulate personal information? If so, should secrecy provisions:

(a) refer to, or use the terminology of, the *Privacy Act*?

(b) allow individuals to access and correct personal information about themselves?

7–5 In what situations is it appropriate for secrecy provisions to authorise handling of personal information where that handling would otherwise breach the *Privacy Act 1988* (Cth)?

7–6 What concerns arise from the interaction between secrecy provisions and data-matching laws and practices? How should these issues be addressed?

7–7 Does the relationship between secrecy provisions and the *Archives Act 1983* (Cth) need to be clarified? If so, how?

7–8 Are there any other concerns about the interaction of secrecy provisions with other legislation regulating the handling of Commonwealth information?

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.

1.2 Such a review was recommended by the ALRC in three prior inquiries. First, in 1995, the ALRC and the Administrative Review Council recommended that a thorough review of all Commonwealth legislative provisions prohibiting disclosure of government-held information by public servants be conducted to ensure that such provisions did not prevent the disclosure of information that was not exempt under the *Freedom of Information Act 1982* (Cth) (FOI Act).[1]

1 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.

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

> The Australian Government should review all legislative and regulatory provisions giving rise to a duty not to disclose official information—including in particular regulation 2.1 of the *Public Service Regulations*—to ensure the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.[2]

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

> The Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.[3]

1.5 These recommendations for a review of secrecy laws were prompted in large measure by the number and diverse range of secrecy provisions. The lack of consistency among the many provisions was remarked upon in 1991 by Paul Finn:

> When one amalgamates the plethora of statutory provisions, regulations, codes, administrative instructions and common law rules one is left in almost every Australian jurisdiction with an ill-fitting, sometimes unintelligible mosaic of prescriptions and proscriptions. For the individual official the consequence of this can be conflicting, sometimes quite unacceptable, legal demands: the trivial can be criminalised, the important left in a state of lamentable uncertainty.[4]

1.6 There are several intertwined issues in Finn's observations that provide a relevant backdrop to this Inquiry. First, a basic practical matter is to identify the 'plethora' of provisions, introduced at different times with different language and different penalties. Such a task is a necessary preliminary to a consideration of the questions of consolidation and modernisation posed in the Terms of Reference—'without that work it's a wilderness', as remarked in an early consultation.[5] To this end, the ALRC is undertaking a 'mapping' exercise to provide a thorough picture of all relevant provisions and to provide a basis for comparison and analysis throughout the Inquiry.

1.7 Secondly, a key challenge is to identify the core principles or values underpinning the 'mosaic of prescriptions and proscriptions' and to distinguish these from the values in play in relation to other Commonwealth provisions concerning information.

---

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

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

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

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

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

1.9 As a preliminary discussion for matters that follow in the remainder of the Issues Paper, this Chapter considers the context for secrecy provisions, relevant definitions and the scope of the Terms of Reference for this Inquiry, and some possible directions for reform.

Context for 'secrecy'

Continuum of provisions

1.10 Secrecy provisions are one way in which the flow of government information can be regulated. So too are the mechanisms for classifying information according to different levels of security under the *Australian Government Protective Security Manual* (PSM).[6] A number of other existing legislative regimes also regulate access to government information. At the federal level these include the *Privacy Act 1988* (Cth) (*Privacy Act*) and the FOI Act. The regime established by the *Archives Act 1983* (Cth) for the storage of, and public access to, government records is also relevant.[7]

1.11 Broadly speaking, the secrecy provisions were introduced first, and imposed obligations on public servants to maintain the confidentiality of their work. Later developments in administrative law during the 1980s saw the introduction of legislation that facilitated greater openness of government information, in the FOI Act; but also provided for the protection of personal information through the *Privacy Act*. Complementing this legislation was the *Archives Act* which signalled a period after which certain documents should be released into the public domain.

---

6 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual* (2005).

7 The ALRC has considered a number of these issues in the past: Australian Law Reform Commission *Privacy and Census*, ALRC 12 (1979); Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995); Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998); Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004); Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008).

1.12 Terms like 'secrecy' and 'openness' are not precise terms and are difficult to define except in broad ways. As Greg Terrill commented:

> The best way to think about them is not to try to arrive at precise definitions. Many have tried this, but no accepted formula has emerged.[8]

1.13 Secrecy, freedom of information, privacy and archives legislation are underpinned by certain understandings of the relationship of government and government officers to information. The relationship of other legislation to secrecy provisions is considered in Chapter 7.

1.14 The ALRC has been asked to consider the secrecy provisions in Commonwealth laws in view of the desirability of having comprehensive, consistent and workable laws and practices in relation to the protection of Commonwealth information. In order to do so the ALRC is considering secrecy provisions in their broader context, including in relation to the other laws with which they sit.

Open government

1.15 At first glance, the value of openness in government appears to be in conflict with the value of maintaining secrecy with respect to government information. Both values reflect certain historical understandings of the relationship between a government, its citizens, its officials and information. The history of secrecy laws is considered briefly in Chapter 2.

1.16 It is said that a central tenet of a modern representative democracy is that the government is open to account for its actions, policies and administrative decisions. A key part of this accountability is public access to the information on which action and policies are based.[9] As Rocque Reynolds has argued:

> Governments have access to, and control of, vast amounts of information which may be personal, commercial, sensitive, confidential or politically and socially significant. How governments collect, store, use and disclose this information; whether the public has access to such information; and when governments are required to generate or provide information to the public, tells us a lot about the relationship between the state and its citizens.[10]

1.17 The idea of 'openness', however, is relatively new to 'Westminster' democracies. The so-called 'Westminster system' was a closed one, based upon a ministerial system of responsibility in which secrecy in relation to the mechanisms of advising ministers, including a permanent civil service, was critical.

> 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

---

8 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 4.

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

10 R Reynolds, 'Obtaining Reasons for Government Decision-Making, FOI and Privacy' in R Creyke and J McMillan (eds), *Control of Government Action* (2005), 891, [18.1.1].

> 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.[11]

1.18 During the early 1970s a number of government committees were set up federally and in some of the Australian states to examine the review of administrative decisions in light of the growing impetus towards openness—particularly influenced by developments in this regard in the United States and in contrast to the adherence to a more closed system of government in the United Kingdom. The legislative reforms that followed became known as the 'new administrative law', the purpose of which was to facilitate effective public administration while at the same time safeguarding the civic rights of the individual citizen.[12] In other words, the aim was to achieve a better balance between secrecy, privacy and openness.

1.19 The 'new administrative law' package included the *Ombudsman Act 1976* (Cth), the *Administrative Appeals Tribunal Act 1975* (Cth) and the *Administrative Decisions (Judicial Review) Act 1977* (Cth). To this was added in the 1980s the FOI Act, the *Archives Act* and the *Privacy Act*.

1.20 The enactment of the FOI Act in particular was considered a 'major step in establishing open government' and a significant step towards overturning 'a deeply entrenched tradition of government secrecy'.[13] The Terms of Reference ask the ALRC to have regard to the importance of balancing the need to protect Commonwealth information and the public interest in an open and accountable system of government. The latter public interest is reflected in the FOI Act, the long title of which emphasises its focus on access: 'An Act to give to members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies'.

1.21 That 'the members of the public' include an increasing group of 'Net Geners'—the 12- to 30-year old cohort or 'Net Generation'—adds a further imperative of openness:

> To win the trust of Net Geners, governments have to be transparent … At a minimum, policy makers should publicize their overall goals and objectives and, for specific issues and decisions, the documents they relied on, the names of the participants in the

11 Freedom of Information Independent Review Panel, *Enhancing Open and Accountable Government: Review of the Freedom of Information Act 1992*, Discussion Paper (2008), 158.
12 M Patterson, *Freedom of Information and Privacy in Australia* (2005), 3–4.
13 Ibid, 3.

> decision-making process, and their underlying rationales and criteria, and they should provide reasons why alternative policy options have not been pursued.[14]

1.22 The move away from a closed to a more open system is also evident in the United Kingdom—the home of the Westminster system—in its introduction of the *Freedom of Information Act 2000*, which came into force in January 2005. To assist in preparation for the operation of the Act and to facilitate its implementation once in effect, the Office of Information Commissioner was established. The Office has a dual purpose—'to promote access to official information and protect personal information'.[15]

1.23 Always balanced against the desirability of open government, however, is the legitimate public interest in protecting some information from disclosure. Government information may need to be protected because it relates to national security or international relations; because it is personal information about an individual; or is information which would be of unfair benefit to a person were it disclosed. The attack on the World Trade Center in New York on 11 September 2001 also had an impact on the security environment and heightened the debate about the 'need to share' information between agencies. In the current security environment some agencies have had to work more closely together, and in different ways than they have in the past. A number of agencies may have different pieces of information which, if connected, might assist in relation to counter-terrorism investigations. In this context, there is a tension in the handling of information between a 'need to know' and a 'need to share'.

1.24 Secrecy provisions approach Commonwealth information from the perspective of the obligation of non-disclosure and the consequences for a Commonwealth officer of breaching such obligations. The *Privacy Act* adds a further perspective in the information continuum. It aims to protect personal information about individuals and give them some control over how that information is collected, stored, used and disclosed. It also gives individuals rights of access to and correction of their own personal information.[16] Secrecy and privacy provisions intersect where personal information is in the hands of a person subject to an obligation of secrecy. In such cases, the person to whom the information relates has rights in relation to the information under privacy law; and the person or agency in whose hands the information resides has responsibilities towards it under privacy principles and obligations not to disclose it both under privacy law and secrecy provisions.

---

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

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

16 The ALRC recently conducted a major inquiry into Australian Privacy Laws: see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008).

Other laws

1.25 Disclosure of government information is not only regulated by legislation. By virtue of the implied right to freedom of political communication, the *Australian Constitution* has an impact on attempts to restrict the dissemination of information. Government information may also be protected through the common law duties of confidentiality and fidelity arising from the employee/employer relationship between the Government and Commonwealth officers.[17] There are also two other ways in which government information may be protected in the context of court or tribunal proceedings—through the mechanisms of public interest immunity claims and ministerial certificates. Each will be considered in turn.

The Constitution

1.26 The *Australian Constitution* establishes a federal system of government in which powers are distributed between the Commonwealth and the six states. The *Constitution* also sets out a list of subjects about which the Australian Parliament may make laws. A number of these provisions could be relied upon to provide the constitutional basis for laws dealing with the confidentiality or secrecy of official government information. Section 52, for example, makes clear that the Australian Parliament has exclusive power to make laws on matters relating to Australian Government public service departments.[18]

1.27 The Australian Parliament also has power to make laws that are incidental to the execution of other powers conferred on it.[19] Thus, while the Parliament has express power to make laws concerning, for example, the federal public service, taxation,[20] defence[21] and the census,[22] it may also make laws that are incidental to these matters. Laws dealing with the confidentiality or secrecy of tax, defence, census or other official information might be construed either as laws relating to the public service, tax, defence or the census, or as incidental to these matters.

1.28 There are, however, a number of constitutional requirements that affect the power of the Australian Parliament to legislate in this area, including the implied constitutional guarantee of freedom of communication about government and political matters.[23] In *Bennett v President, Human Rights and Equal Opportunity Commission*,[24] Finn J considered the relationship between the implied freedom and provisions

17 The meaning of 'Commonwealth officer' is considered below.
18 *Australian Constitution* s 52(ii).
19 Ibid, s 51(xxxix).
20 Ibid, s 51(ii).
21 Ibid, s 51(vi).
22 Ibid, s 51(xi).
23 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
24 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119 (*Bennett*).

regulating the disclosure of official information, in particular regulation 7(13) of the *Public Service Regulations 1999* (Cth), which stated that:

> An APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head's express authority, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge.[25]

1.29 Finn J found the regulation to be inconsistent with the implied freedom of political communication and declared it to be invalid. He assessed the regulation against the test established by the High Court in *Lange v Australian Broadcasting Corporation*:[26] first, whether the regulation burdened freedom of communication about government or political matters; and secondly, if so, whether the regulation was reasonably appropriate and adapted to serve a legitimate end, the fulfilment of which was compatible with the maintenance of the system of representative and responsible government prescribed by the *Australian Constitution*.

1.30 With respect to the first matter, Finn J found that the regulation burdened freedom of political communication by regulating the disclosure by public servants of information about the 'public business' of the Australian Government. With respect to the second, he held that the regulation was not reasonably and appropriately adapted to serve a legitimate end. He described it as a 'catch-all' provision, which did not differentiate between the types of information protected or the consequences of disclosure.

> 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.[27]

1.31 Regulation 7(13) and its successor, which was in similar terms, have now been repealed and replaced by reg 2.1. The new regulation—expressly limited to situations in which it is reasonably foreseeable that disclosure of official information could be prejudicial to the effective working of government—is discussed in detail in Chapter 3. It was considered by Refshauge J, of the ACT Supreme Court, in *R v Goreng Goreng*.[28] Refshauge J rejected the argument that the new regulation was inconsistent with the implied constitutional freedom of political communication. His decision was

---

25 *Public Service Regulations 1999* (Cth) reg 7(13), now repealed and replaced.
26 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
27 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119, 141.
28 *R v Goreng Goreng* [2008] ACTSC 74.

based on the fact that the new regulation was much more limited and targeted than its predecessors, and focused on the protection of a legitimate interest, that is, the effective working of government,[29] thus satisfying the test in *Lange v Australian Broadcasting Corporation*.[30]

1.32 Richard Jolly has expressed the view that the implied freedom may also provide some constitutional protection for so-called 'whistleblowers'—those Commonwealth officers who deliberately breach secrecy obligations to draw attention to perceived corruption or maladministration within Government:[31]

> The protection could also extend to other actions taken by the government against such persons, either to prevent disclosure or to punish them, and it is unlikely that any public interest would justify the complete prohibition on disclosure of misconduct or corruption. If actions such as the commencement of prosecution, an application for an injunction, the taking of disciplinary action against an employee or the enforcement of contractual restrictions on disclosure are characterised as the exercise of executive power, those actions could themselves be constitutionally invalid if they result in the unjustified curtailment of the freedom to communicate. As these measures seem to subject the person to 'legal control' the implied freedom may provide some measure of immunity for the whistleblower from legal or disciplinary action. This may be an area where the operation of the implied freedom on executive power is significant.[32]

1.33 In addition, Jolly noted that the equitable duty of confidentiality owed to government as an employer seems consistent with the implied freedom of political communication, as the protection offered by the equitable duty is limited to situations in which disclosure is likely to damage the public interest.[33] This is discussed further below.

1.34 As noted at the beginning of this chapter, in ALRC 98 the ALRC recommended that reg 2.1 in particular should be included in the proposed review of secrecy provisions:

> … to ensure that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.[34]

1.35 Chapters 2 and 3 consider these issues in more detail and test a range of provisions that regulate the disclosure of official information against the principles set

---

29 Ibid, [37].
30 *Lange v Australian Broadcasting Corporation* (1997) 189 CLR 520.
31 See the definition of 'whistleblower' below.
32 R Jolly, 'The Implied Freedom of Political Communication and Disclosure of Government Information' (2000) 28 *Federal Law Review* 42, 48.
33 Ibid, 49.
34 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–2.

out by Finn J in *Bennett*. Chapter 4 looks at the protection of whistleblowers in the context of a review of exceptions and defences to secrecy provisions.

Equitable action for breach of confidence

1.36 An action for breach of confidence in equity may be used to restrict the disclosure of information in certain circumstances. In the High Court case of *Commonwealth v Fairfax*,[35] Mason J cited with approval the following formulation of the principle of breach of confidence:

> 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'.[36]

1.37 Unlike an action in copyright, an action for breach of confidence may be taken in relation to information itself, whether written or verbal. An action can also be brought against a third party to whom information has been communicated in breach of a duty of confidence where that third party was aware, or should reasonably have been aware, that the information was confidential.

1.38 *Commonwealth v Fairfax* gave rise to the question of the applicability of the doctrine of breach of confidence in the context of disclosure of government information and the availability of an injunction in such a case. *The Age* and *The Sydney Morning Herald* newspapers were proposing to publish extracts from an upcoming book, *Documents on Australian Defence and Foreign Policy 1968–1975*,[37] including extracts from classified government documents dealing with the ANZUS Treaty and the East Timor crisis. Copies of the early editions of the newspapers had been distributed before the publishers received notice of the interim injunction restraining publication. Mason J concluded that the information had probably been leaked by a public servant in breach of his or her duty and contrary to the security classifications marked on some of the documents.[38]

1.39 Mason J commented that although the equitable action for breach of confidence was developed 'to protect the personal, private and proprietary interests of the citizen, not to protect the very different interests of the executive government',[39] he accepted that in some circumstances the principles could be applied to protect information in the hands of government. To do so it must be shown

> not only that the information is confidential in quality and that it was imparted so as to import an obligation of confidence, but also that there will be 'an unauthorised use of that information to the detriment of the party communicating it'. The question then,

---

35 *Commonwealth v Fairfax* (1980) 147 CLR 39.
36 Ibid, 50, citing Swinfen Eady LJ in *Lord Ashburton v Pope* (1913) 2 Ch 469, 475.
37 G Munster and J Walsh, *Documents on Australian Defence and Foreign Policy 1968-1975* (1980).
38 Security classifications are considered in Ch 6.
39 *Commonwealth v Fairfax* (1980) 147 CLR 39, 51.

> when the executive government seeks the protection given by equity, is: What detriment does it need to show?[40]

1.40 The conclusion drawn in the case was that disclosure of confidential information would be restrained at the instance of the Government if it appeared that disclosure would be 'inimical to the public interest because national security, relations with foreign countries or the ordinary course of business of government will be prejudiced'. The decision noted that:

> it can scarcely be a relevant detriment to the government that publication of material concerning its actions will merely expose it to public discussion and criticism. It is unacceptable in our democratic society that there should be a restraint on the publication of information relating to government when the only vice of that information is that it enables the public to discuss, review and criticize government action.
>
> Accordingly, the court will determine the government's claim to confidentiality by reference to the public interest. Unless disclosure is likely to injure the public interest, it will not be protected.[41]

1.41 The importance of public discussion was reiterated by the High Court in *Attorney-General (UK) v Heinemann Publishers Australia Pty Ltd*, where it referred to the 'public interest in freedom of information and discussion'.[42]

1.42 As noted above, this results in a consistent approach to the doctrine of confidentiality and the implied freedom of political communication. In Jolly's view:

> to the extent that secrecy law burdens the implied freedom by preventing disclosure in some cases, the balancing of the competing legitimate public interests of government in non-disclosure, and the freedom of communication in disclosure, would seem to ensure that the law is no more than is reasonably appropriate and adapted to achieve legitimate government objectives.[43]

1.43 The duty of confidentiality may also have application in circumstances where the government has a contractual relationship with a private provider of a government service (for example, a provider of an aged care service).[44] In addition, confidentiality clauses are included in many government contracts with service providers as a matter of course.[45] Information held by government contractors that is categorised as

---

40 Ibid, 51, notes omitted.

41 Ibid, 52.

42 *Attorney-General (UK) v Heinmann Publishing Australia Pty Ltd* (1988) 165 CLR 30, 45.

43 R Jolly, 'The Implied Freedom of Political Communication and Disclosure of Government Information' (2000) 28 *Federal Law Review* 42, 49.

44 J Macken, P O'Grady, C Sappideen and G Warburton, *Law of Employment* (4th ed, 2002), 141.

45 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 53. Secrecy provisions may also expressly apply to contractors: see Ch 3.

'commercial in confidence', subject to a confidentiality clause or to restraint from publication by the duty of confidence, may therefore be subject to a higher level of protection than information held within government.[46]

Common law duty of fidelity and loyalty

1.44 The common law imposes on any employee the duty of fidelity and loyalty (or good faith). This duty arises from the contract of employment,[47] but may also arise from a fiduciary obligation where the employee is in a special position of trust and confidence.[48] The duty of fidelity has largely been imposed in situations involving confidential information and has been expressed as meaning that an employee must not use information obtained in the course of his or her employment to the detriment of the employer.[49]

1.45 In his report *Integrity in Government: Official Information*, Finn noted that the effect of the duty of fidelity on a public servant is more complicated than in the case of a private sector employee, as public servants have a duty to their employer as well as an overriding duty to the public at large.

> For this reason, and as with the law of confidentiality as it applies to governmental information, the 'public interest' and not merely the 'employer's interests', can affect incidents of the duty itself.[50]

1.46 Finn noted that the formulation of the duty is necessarily imprecise. This is because of the variety of considerations that must be brought to bear on the question of the propriety or otherwise of the use including:

> the nature of the information and whether or not it is publically 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.[51]

1.47 In *Bennett*, Finn J made a number of comments about whether a direction not to disclose information could be supported by the public servant's duty of fidelity and loyalty as an employee.[52] He noted that the features of the duty were dependent on the facts in each case, and that public sector employees may have different demands placed upon them by virtue of their position.

> The difficulty this creates … is that there is no significant jurisprudence on how the duty is to be adapted to accommodate the distinctive demands of public service

---

46 For example, documents relating to business affairs are exempt from the *Freedom of Information Act 1982* (Cth) s 43. See also Ch 7.

47 *Robb v Green* [1895] 2 QB 315.

48 J Macken, P O'Grady, C Sappideen and G Warburton, *Law of Employment* (4th ed, 2002), 139–141.

49 *Faccenda Chicken v Fowler* [1986] 1 All ER 617, 136–137.

50 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 204.

51 Ibid, 205–206.

52 It should be noted that this issue was remitted back to HREOC: *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119, 145.

> 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 the 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.[53]

1.48 Finn J referred to Canadian jurisprudence and particularly the conclusion of the Supreme Court of Canada in *Fraser v Public Service Staff Relations Board*[54] that, in relation to comments critical of the government, the Court must balance the right of an individual, as a member of the Canadian community, to speak freely on issues of public importance against the duty of that individual, as a public servant, to fulfil his or her functions as an employee of the government.[55] 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
- where the comments had no impact on the ability of the employee to perform his or her duties.[56]

1.49 However, the right to comment was not unqualified. Dickson CJ stated that:

> Public servants have some freedom to criticize the Government. But it is not an absolute freedom. To take but one example, whereas it is obvious that it would not be 'just cause' for a provincial government to dismiss a provincial clerk who stood in a crowd on a Sunday afternoon to protest provincial day care policies, it is equally obvious that the same government would have just cause to dismiss the Deputy Minister for Social Services who spoke vigorously against the same policies at the same rally.[57]

1.50 In the later cases of *Osborne v Canada*[58] and *Haydon v Canada*,[59] the Canadian Courts further considered the ability of public servants to comment on government matters in the context of the right of freedom of speech under the *Canadian Charter of Rights and Freedoms*. Section 1 of the Charter guarantees the rights and freedoms set

---

53 Ibid, 145–126.
54 *Fraser v Public Service Staff Relations Board* [1985] 2 SCR 455.
55 Ibid, [34].
56 Ibid, [41].
57 Ibid, [36].
58 *Osborne v Canada* [1991] 2 SCR 69 (*Osborne*).
59 *Haydon v Canada* [2001] 2 FC 82 (*Haydon*).

out in it subject to 'such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society'.[60]

1.51 In *Osborne*, the Supreme Court followed the reasoning in *Fraser*, stating that restrictions on the rights of public servants to comment on government matters should be based on the level of seniority of the employee, including whether he or she participated in policy development or managerial decisions. This distinction allowed most public servants to participate freely in public discourse, while still maintaining the neutrality of the public service overall.[61]

1.52 In *Haydon*, the Federal Court held that the common law duty of fidelity and loyalty provided a reasonable limit on freedom of expression within the Charter and cited with approval the three exceptions outlined in *Fraser* (above), where disclosure or comment would be allowed. In *Haydon*, the disclosures related to drug approval processes for bovine growth hormones. The Court found that the issue of the safety of growth hormones was 'a legitimate public concern requiring a public debate' and that 'the common law duty of loyalty does not impose unquestioning silence'.[62] It was also an important feature of that case that attempts had been made to resolve the issues internally before public comments were made.

1.53 In *Read v Canada*[63] the Federal Court acknowledged that while there could be other specific exceptions to the duty in addition to those enunciated in *Fraser*, there was no generalised 'public interest' exemption. Harrington J rejected the proposition that *Haydon* had created a more general exception, finding that the public concern in that case was specifically a danger to the health and safety of persons and therefore within the exceptions identified in *Fraser*.[64]

1.54 Christopher Erskine SC has suggested that the Canadian cases set out a principled basis upon which a balancing process can be undertaken to determine when the right of a public servant to comment outweighs their duty to the effective functioning of government.[65] He considers that the common law duty of fidelity 'has coherent and sensible principles that neatly cover the difficult questions raised by public servants disclosing information'.[66]

1.55 Are these principles applicable in the Australian context? As Finn J noted in *Bennett*, there is little law on how the duty of fidelity applies to public servants in Australia. If the Canadian principles were applied there is a question whether the duty

---

60 This is similar in effect to the limitation of the implied freedom of political communication in the *Australian Constitution* discussed above.
61 *Osborne v Canada* [1991] 2 SCR 69, 99.
62 *Haydon v Canada* [2001] 2 FC 82, [120].
63 *Read v Canada* [2005] FC 798.
64 Ibid, [107]–[108].
65 C Erskine, 'The Bennett Decision Explained: The Sky is not Falling!' (2005) 46 *Australian Institute of Administrative Law (AIAL) Forum* 15, 24.
66 Ibid, 1.

under reg 2.1 of the *Public Service Regulations* and the consequent general offence under s 70 of the *Crimes Act* are necessary. Would the common law principles cover the field to provide sufficient protection of Commonwealth information?

1.56 Erskine outlines a number of reasons why the common law framework might be preferable to the duty imposed by the regulation or other statutory provisions, including that:

- the duty of fidelity is compatible with the implied freedom of political expression, as it is based on a 'reasonableness test';[67]
- the duty is not absolute but is tailored to what is fair in the circumstances of each case, thereby allowing the imposition of a higher duty where, for example, the public servant is a senior officer or where the information concerns matters of national security; and
- the duty does not prevent disclosure on matters of public health and safety or illegality.

1.57 Erskine suggests that, as a general rule, a public servant should raise concerns internally before making public comment. This provides some protection for 'whistleblowers', which is currently absent from the regulation.[68]

1.58 The ALRC is interested in hearing views on whether the common law principles are sufficient and appropriate of themselves to regulate disclosure of Commonwealth information by public servants.

Public interest immunity

1.59 A claim of public interest immunity (also called state interest immunity) is one of the most common ways in which government information can be protected in court proceedings and may be made both under the common law and under s 130 of the *Evidence Act 1995* (Cth).[69] A claim of public interest immunity differs from other mechanisms to protect sensitive evidence in that it operates to exclude the information completely, rather than limiting or protecting its disclosure to the public or parties to the proceedings while it is being used in court.

---

67 This issue is discussed further in Ch 3.

68 C Erskine, 'The Bennett Decision Explained: The Sky is not Falling!' (2005) 46 *Australian Institute of Administrative Law (AIAL) Forum* 15, 24–25. Whistleblowing is discussed further in Ch 4.

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

1.60 The common law formulation of public interest immunity is stated in *Sankey v Whitlam*:

> [T]he court will not order the production of a document, although relevant and otherwise admissible, if it would be injurious to the public interest to do so.[70]

1.61 In essence, public interest immunity invokes a balancing test. When successful, courts limit the disclosure of information or documents on the basis that the public interest against disclosure outweighs the need for disclosure to ensure justice in a particular case.

1.62 Hunter, Cameron and Henning note that the grounds for what constitutes public interest under the common law are not closed, but generally relate to the interests of central government.[71] Claims for public interest immunity are most commonly made by the government in relation to Cabinet deliberations, high level advice to government, communications or negotiations between governments, national security, police investigation methods, and in relation to the activities of Australian Security and Intelligence Organisation (ASIO) officers, police informers, and other types of informers or covert operatives.[72]

1.63 Section 130 of the uniform Evidence Acts applies the immunity to 'matters of state':

> (1) If the public interest in admitting into evidence information or a document that relates to matters of state is outweighed by the public interest in preserving secrecy or confidentiality in relation to the information or document, the court may direct that the information or document not be adduced as evidence.

1.64 In *Keeping Secrets* (ALRC 98), the ALRC examined the operation of s 130 in the context of protection of classified and security sensitive information in court proceedings. It was estimated that public interest immunity arises as an issue in less than one per cent of cases across all courts.[73] The ALRC also found that the public interest immunity procedure works effectively, although some submissions suggested that the procedures for invoking its use required clarification.[74] In *Uniform Evidence Law* (ALRC 102), the ALRC confirmed its view that the procedures for invoking s 130 in court work well.[75]

Ministerial certificates

1.65 The issuing of ministerial certificates in order to claim public interest immunity was common in the United Kingdom and Australia until the 1960s. In 1942, the House

---

70 *Sankey v Whitlam* (1978) 142 CLR 1, 38 (Gibbs ACJ).
71 J Hunter, C Cameron and T Henning, *Litigation I: Civil Procedure* (7th ed, 2005), [8.102].
72 Ibid, [8.102].
73 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [8.192].
74 Australian Law Reform Commission, *Evidence* (1985), [8.192]–[8.205].
75 Australian Law Reform Commission, *Uniform Evidence Law* (2005), [15.158].

of Lords made a controversial decision—in the context of a world war—that courts should accept without question a certificate issued by a minister certifying the Government's view that the document or secret should be excluded in the public interest.[76]

1.66 In the UK, this doctrine was later overturned in *Conway v Rimmer*.[77] This case established that a minister's certificate was no longer able to protect information in and of itself, and that a trial judge had to balance the state interest against the broader public interest. This approach has continued to be expanded in the UK cases. In *Air Canada v Secretary of State for Trade (No 2)*,[78] the House of Lords made it clear that even Cabinet papers regarding government policy would not be immune from disclosure where their contents went to the heart of the matter at issue.

1.67 In Australia, *Sankey v Whitlam* established that, as a matter of common law, ministerial certificate claims were not regarded as conclusive, with the court placed in the role of the ultimate guardian of public policy to ensure justice in each case.[79]

1.68 However, conclusive certificates are part of the current statutory regime for exempting certain types of information from release under the FOI Act.[80] Under s 33(2) of that Act, a conclusive certificate may be issued by the relevant Minister which exempts a document from disclosure under the Act on the basis, for example, that it relates to national security, defence or international relations.[81]

1.69 Under s 55 of the FOI Act, an appeal may be taken to the Administrative Appeals Tribunal (AAT) to review the issuing of a conclusive certificate. The role of the AAT in reviewing these certificates is not the same as the role of the courts in a public interest immunity case since the AAT does not consider whether the public interest in disclosure outweighs the public interest in non-disclosure. Rather, the AAT

---

76 See *Duncan v Cammell, Laird & Co* [1942] AC 264.

77 *Conway v Rimmer* [1968] AC 910.

78 *Air Canada v Secretary of State for Trade* [1932] 2 WLR 252.

79 *Sankey v Whitlam* (1978) 142 CLR 1, 38–39 (Gibbs ACJ).

80 Freedom of information is discussed in more detail in Ch 6. The Cabinet Secretary and Special Minister for State, Senator the Hon John Faulkner, has stated that the Australian Government will introduce a Bill to remove the power to issue conclusive certificates in FOI and archives legislation before the end of 2008, and will release an exposure draft bill for further FOI reform early in 2009: J Faulkner (Cabinet Secretary and Special Minister for State), 'Freedom of Information Reform' (Press Release, 22 July 2008).

81 As outlined in s 33(1) of the FOI Act. Conclusive certificates may also be issued in relation to information about Commonwealth/State relations (s 33A), Cabinet documents (s 34), Executive Council documents (s 35) and internal working documents which show government deliberations or processes (s 36). The leading case on conclusive certificates is *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423. In *McKinnon*, the majority of the High Court found that if one reasonable ground exists for the claim that the release of the information would not be in public interest, the conclusiveness of a certificate will be beyond review by the AAT. This will be the case even where there are also reasonable arguments that can be made for the revelation of document in the public interest.

considers whether reasonable grounds exist (at the time of the hearing) for the claims made in the certificate.[82]

1.70 Conclusive ministerial certificates are also allowed in relation to the review of decisions by the Refugee Review Tribunal under s 411(3) of the *Migration Act 1958* (Cth). Under that section, the Minister may issue a conclusive certificate if he or she believes that it would be contrary to the national interest to change the decision or that it would be contrary to the national interest for the decision to be reviewed. Similar conclusive certificates are available regarding decisions of the Migration Review Tribunal under s 339 of the *Migration Act* and the AAT under s 502 of that Act.

1.71 Different types of documents might be issued by an Attorney-General or other minister, all of which have been described as 'certificates', but which have different functions and purposes. For example:

- In contexts outside court and tribunal proceedings, a minister may issue a certificate that bars the production of material that would otherwise have been disclosed. This may block information being given to the public (as under the FOI Act, s 33(2)) or being given to another government official (as under the *Ombudsman Act 1976* (Cth), s 9(3) or the *Privacy Act 1988* (Cth), s 70).

- In court or tribunal proceedings, a claim for public interest immunity will often be supported by an affidavit or other statement sworn or issued by the Attorney-General or other minister asserting the critical nature of the classified or security sensitive information in question to national defence or security.

- In court or tribunal proceedings, the Attorney-General or other minister may issue a certificate, often in exercise of a statutory power to do so, that is (or purports to be) conclusive of the status of, or the way in which the material in question can be used. Another exceptional variety is the certificates that the Minister may issue under s 503A(3) of the *Migration Act*, which authorises the release of material that would otherwise have remained 'confidential'.

1.72 In *Keeping Secrets* (ALRC 98), the ALRC was of the view that, in relation to legal proceedings, no statement issued by a minister in support of a claim to be

---

82 Section 58(4) of the FOI Act states: 'Where application has been made to the Tribunal for the review of a decision to grant access to a document that is claimed to be an exempt document under section 33, 33A, 34 or 35 and in respect of which a certificate (other than a certificate of a kind referred to in subsection 5(A)) is in force under that section, the Tribunal shall, if the applicant so requests, determine the question whether there exists reasonable grounds for that claim'. In *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, the majority of the High Court found that if one reasonable ground exists for the claim that the release of the information would not be in public interest, the conclusiveness of a certificate will be beyond review by the AAT. This will be the case even where there are also reasonable arguments that can be made for the disclosure of the document in the public interest.

determined by a court or tribunal under the proposed Act should be conclusive of that claim or any aspect of it.[83]

Information flows

1.73 In this Inquiry the ALRC has been asked to consider relevant laws and practices relating to the protection of Commonwealth information. The Terms of Reference also have regard to the increased need to share such information within and between governments and with the private sector.[84]

1.74 Information 'underpins almost all of government activity'.[85] As Terrill notes, information is both an 'object in it own right' and 'a dimension of all government activity'. [86] It has also been remarked in past inquiries that:

> On the one hand, an unregulated transfer of information has implications both in terms of privacy and breach of confidence. However, on the other hand, limits on the access of Commonwealth agencies to information may impede the agencies, particularly in relation to law enforcement and revenue protection.[87]

1.75 Ensuring that information is able to 'flow' to the parts of government as needed is a key element of a 'whole-of-government' response to policy making. In its report *Connecting Government*, the Australian Government's Management Advisory Committee[88] defined 'whole of government' in the Australian Public Service (APS) as denoting:

> public service agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues. Approaches can be formal and informal. They can focus on policy development, program management and service delivery.[89]

1.76 As part of this process, information sharing is essential. Information flows may need to take place:

- where there is a crisis or national emergency;

---

83 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [8.241].

84 See Terms of Reference at the front of this Issues Paper.

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

86 Ibid, 5.

87 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 59.

88 The MAC is a forum of Secretaries and Agency Heads established under the *Public Service Act 1999* 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.

89 Australian Government Management Advisory Committee, *Connecting Government: Whole of Government Responses to Australia's Priority Challenges* (2004), 4.

- 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 Australian Taxation Office (ATO) and Centrelink, or between Centrelink and a private employment service provider;

- to manage areas of joint activity by encouraging the sharing of information with the Australian government, across jurisdictions and with the private sector.[90]

1.77 Secrecy laws may affect communication at different points in the information flow. The restricted or proscribed conduct may concern disclosure, or amount to a prohibition on communication in certain circumstances.[91]

1.78 In the 1995 review conducted by the House of Representatives Standing Committee on Legal and Constitutional Affairs, the Committee heard that secrecy provisions frequently impeded the flow of information from one department to another. In its evidence to the Committee, the Attorney-General's Department took the view that secrecy provisions were developed to prevent disclosure of official information to the public, but were too inflexible to meet the changing need to transfer information within government, for example across the taxation, health and social security areas.[92]

1.79 More recently, the Treasury reviewed the secrecy provisions in taxation legislation (the Taxation Secrecy Review) and considered the need to balance taxpayer privacy against the need to facilitate government operations through information flows. In that review, it was noted that law enforcement agencies consider that current secrecy and disclosure provisions hinder the investigation and prosecution of serious crime as taxpayer information provided by the ATO cannot be used as evidence in the prosecution of a non-tax related offence.[93]

1.80 Another issue raised in the Taxation Secrecy Review was whether the Commissioner of Taxation could access records of the employee details of ATO employees. At present, the Commissioner of Taxation, when acting in his or her capacity as an agency head, can only access employee tax information that has been obtained from a public source. A suggestion has been made that an exception be introduced to allow taxation information about ATO officers or contractors to be

---

90 Ibid, 60.

91 For example, while not directly concerning secrecy laws, in formulating Australia's response to the terrorist attacks in Bali in 2002, the sharing of information between agencies was said to be hampered by the operation of the *Privacy Act.* One of the key difficulties was that agencies did not have a shared understanding of how the Act operated, particularly in times of crises: Ibid, 195.

92 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 61.

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

disclosed to the Commissioner in his capacity as their employer. This would allow the Commissioner to be confident that all employees have complied with their tax obligations and thus ensure community confidence in the ATO. [94]

1.81 The ALRC is interested in hearing about the impact of secrecy provisions on the sharing of Commonwealth information within and between governments and the private sector.

Prior reviews

1.82 Commonwealth secrecy laws have been considered in a number of reviews and inquiries, either directly or indirectly. For example, in 1979, the Senate Standing Committee on Legal and Constitutional Affairs was highly critical of the plethora of secrecy laws in Commonwealth legislation. In its report on the Freedom of Information Bill 1978 (Cth) and the Archives Bill 1978 (Cth), the Committee commented that:

> It appears to be a fashionable contemporary drafting practice to insert in every new statute a standard provision making it an offence for an official governed by the statute to disclose without authorisation any information of which he has gained knowledge officially.[95]

1.83 The Committee also noted that many secrecy provisions conflicted diametrically with the philosophy espoused in the Freedom of Information Bill 1978 (Cth).[96]

1.84 In 1983, the Human Rights Commission reviewed the *Crimes Act* and found that s 70 could operate in a manner inconsistent with art 19 of the International Covenant on Civil and Political Rights (freedom of expression). The Commission recommended that s 70 be amended to limit its operation to the kinds of information in respect of which restrictions may be imposed under art 19.3—these being for the protection of national security or public order, or of public health or morals.[97]

1.85 The secrecy provisions themselves have been directly reviewed a number of times. The Gibbs Committee Review of Commonwealth Criminal Law (Gibbs Committee)[98] considered the general secrecy provisions in ss 70 and 79 of the *Crimes Act*, the secrecy provisions contained in specific acts and the operation of the common law. The Committee concluded that:

---

94 Ibid, 29.

95 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), 233.

96 Ibid, 236.

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

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

> 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.[99]

1.86 The Gibbs Committee recommended that ss 70 and 79 of the *Crimes Act* should be repealed, and that:

> the application of criminal sanctions under the general criminal law of the Commonwealth to disclosure of official information should be limited to certain categories of information and that these should be no more widely stated than is strictly required for the effective functioning of Government.[100]

1.87 The Gibbs Committee went on to consider what categories of information should be protected by criminal sanctions. These included information relating to intelligence and security services, defence or foreign relations, and information obtained in confidence from other governments or international organisations.[101]

1.88 In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs considered the operation of ss 70 and 79 and noted the longstanding calls for reform.[102] The Committee identified a number of problems with the sections. These included the lack of precision in the drafting—particularly since the duty not to disclose is not located in the *Crimes Act*—and the application of the sections to officers not employed under the *Public Service Act.*[103] The Committee also noted the lack of consistency in drafting and penalties across the secrecy provisions in other Commonwealth statutes.[104] The Committee recommended that the existing secrecy provisions should be rationalised and consolidated into a general offence within the *Crimes Act*.[105]

1.89 Further, as noted at the beginning of this Chapter, the ALRC has also recommended a review of Commonwealth secrecy provisions in three prior inquiries.[106]

---

99 Ibid, 315.
100 Ibid, 317.
101 Ibid, 317–321.
102 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 90, 91.
103 Ibid, 91–92.
104 Ibid, 95.
105 Ibid, 118.
106 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Commonwealth Freedom of Information Act 1982*, ALRC 77 (1995), Ch 4, 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.

Scope of the Inquiry

Terms of Reference

1.90 The Terms of Reference are reproduced at the beginning of this Issues Paper. The ALRC is directed to focus on 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 Attorney-General of Australia, the Hon Robert McClelland MP, identified four factors as relevant to the decision to initiate the Inquiry:

- 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.

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

a. relevant laws and practices relating to the protection of Commonwealth information, including the scope and appropriateness of legislative provisions regarding secrecy and confidentiality;

b. whether there is a need to consolidate and modernise relevant provisions currently in the *Crimes Act 1914* (Cth) and other Commonwealth legislation for inclusion in the *Criminal Code* (Cth);

c. the way in which secrecy laws in the Crimes Act interact with other laws and practices, including those relating to secrecy, privacy, freedom of information, archiving, whistle-blowing, and data-matching;

d. whether there should be different considerations for secrecy laws relating to the protection of national security and other sensitive Commonwealth information; and

e. any related matter.

Definitions

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

Secrecy laws

1.93 A key preliminary step in this Inquiry is to identify what provisions are included in the concept of secrecy provisions.

1.94 Commonwealth secrecy provisions and the information they protect are varied. Some provisions are quite specific, and prohibit the disclosure of identified classified, sensitive or personal information. There are also, however, offences of general application that prohibit disclosure of *any* information a government officer has obtained in their official capacity.

1.95 McGinness has noted that:

> With the expansion of the Commonwealth's role after the mid-1940s in areas such as taxation, health, education, welfare, scientific research, industry assistance and regulation, secrecy provisions increased in number as a reflection of the increase in personal and commercially sensitive information collected by the government.[107]

1.96 The ALRC has indentified a wide range of secrecy provisions across a range of Acts and regulations that reflect this expansion. Chapter 2 provides an overview of secrecy provisions in federal legislation and their historical development.

1.97 There is no established definition of the term 'secrecy law' or 'secrecy provision'. In reviewing the range of provisions that should be considered in this Inquiry, the ALRC has identified, for example, provisions that deal with communicating or disclosing information; provisions about receiving information that is secret; and those concerning misuse of information. Issues of secrecy are also aspects of the management of information in an administrative sense as well as being the subject of specific prescription in legislation.

1.98 In this Inquiry, the ALRC refers to a secrecy provision as one in an Act or subordinate legislation. Aspects of practice and procedure regarding the protection of information and management of information handling are also relevant and are considered separately in Chapter 6.

1.99 The ALRC considers that the concept of a secrecy provision is one that has as its principal focus the protection of information through obligations of confidentiality or secrecy. Such provisions are not limited to restricting disclosure of information. They may cover a chain of conduct that leads to possible disclosure—such as soliciting, obtaining, copying, using, retaining, divulging, and communicating information. They also may include provisions dealing with receipt of disclosed information. All the provisions identified, however, are focused on protecting the confidentiality of the information.

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

---

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

- prohibit the misuse of information for personal gain—as the principal concern of such provisions is fraud, not protection of the confidentiality of the information;[108]

- concern the storage, modifying or destroying of information; and

- that permit the disclosure of, for example, personal information in certain circumstances—as the core aim concerns privacy of personal information.

1.101 For the purposes of this Inquiry, therefore, the ALRC has defined the concept of a secrecy law broadly as any provision in primary or subordinate legislation which imposes secrecy or confidentiality obligations relating to the handling of Commonwealth information. 'Commonwealth information' (sometimes referred to as 'official information')—considered further below—is information developed, received or collected by or on behalf of the Commonwealth government.

Commonwealth information

1.102 Commonwealth information (which may also be called 'government information' or 'official information') is information developed, received or collected by or on behalf of the Commonwealth government. It includes information the Commonwealth receives from individuals (such as personal information provided to an agency like Centrelink), information developed in-house (for example, intelligence reports) and information generated by foreign governments that is shared with the Commonwealth government.

1.103 Commonwealth information may be classified into a number of categories based upon their 'sensitivity'. The *Australian Government Protective Security Manual* (PSM) binds all Commonwealth agencies to a series of procedures designed to protect Commonwealth information, including classified information and other sensitive information.

1.104 Once information is classified, it is marked accordingly and given various forms of protection—including restricting access to people with a security clearance at the appropriate level; physical protection, such as storage in approved containers of sufficient strength or meeting other security standards; and restrictions on how it may be transferred from one person to another. Chapter 6 discusses in detail the PSM and

---

108 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.

other manuals, policies and guidelines relating to information handling to which Commonwealth officers (and other persons made privy to Commonwealth information) are subject. The protection of classified and security sensitive information was also considered by the ALRC in *Keeping Secrets* (ALRC 98).[109]

1.105 Outside the classification process, documents prepared for use by the Commonwealth Cabinet to formulate policy and make decisions are given special protection on the basis that unauthorised disclosure would damage the fullness and frankness of discussions in the Cabinet Room and would thereby inhibit the process of good government. These documents are marked Cabinet-in-Confidence regardless of any other security considerations. The Cabinet Handbook stipulates that Cabinet-in-Confidence documents require a level of protection at least equivalent to that given to documents classified as 'Protected' under the guidelines set out in the PSM.[110]

1.106 As discussed above, certain legislation—most notably the FOI Act—gives the public rights of access to government-held or government-controlled information, subject to a number of exceptions and exemptions.[111] However, the fact that information is neither classified nor a Cabinet document does not mean that it is freely available. Other legislation or the common law duty of confidence may also protect Commonwealth information in certain circumstances.

Commonwealth officer

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

1.108 The *Crimes Act 1914* (Cth) includes a general prohibition against the unauthorised disclosure of official information by current and former Commonwealth officers.[112] 'Commonwealth officers' are defined as including those appointed or engaged under the holding office under the *Public Service Act 1999* (Cth), those holding office under the Commonwealth, and those who perform services by or on behalf of the Commonwealth.[113]

1.109 The *Public Service Act* refers to Australian Public Service (APS) employees, and includes those employed in Australian Government departments and statutory agencies. 'Commonwealth officer', defined in the *Crimes Act*, includes, but is wider than, 'APS employees'. These definitions are discussed in more detail in Chapter 3.

---

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

110 Australian Government Department of the Prime Minister and Cabinet, *Cabinet Handbook* (5th ed, 2004), 28, [7.5].

111 See Ch 7.

112 *Crimes Act 1914* (Cth) s 70.

113 Ibid s 3.

1.110 For the purposes of this Issues Paper, the wider expression is used unless the context requires a narrower term.

Whistleblower

1.111 The term 'whistleblower' is of relatively recent origins. The Macquarie Dictionary suggests that the term emerged in the United States in the second half of the 1960s from the phrase 'blow the whistle on'. It is now commonly used even in official contexts, as for example in the Inquiry into Whistleblower Protection announced by the Cabinet Secretary and Special Minister for State, Senator the Hon John Faulkner, on 11 July 2008.[114]

1.112 In this Issues Paper, the term 'whistleblower' is used to refer to someone who makes a public interest disclosure, for example, alleging that the conduct of a Commonwealth officer or agency is corrupt or involves maladministration. This topic is discussed in greater detail in Chapter 4.

Matters outside this Inquiry

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

1.114 The ALRC's approach in this Inquiry is to concentrate on those secrecy laws that prohibit disclosure to persons other than courts and tribunals. This means that the ALRC will be considering both the scope and appropriateness of current secrecy provisions—and how they affect the ability of information to flow between agencies, governments, and with the private sector.

1.115 These provisions concern the secrecy and confidentiality obligations of individual Commonwealth officers (or other people nominated in legislation) and the information they acquire by virtue of their position. Therefore review of the government's larger security and information management systems is outside the scope of this Inquiry.

---

114 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Inquiry into Whistleblowing Protections Within the Australian Government Public Sector: Terms of Reference* (2008) Parliament of Australia.

1.116 In ALRC 98, the ALRC considered the protection of classified and security sensitive information in the context of court and tribunal proceedings.[115] 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).[116]

1.117 As noted above, the ALRC has also considered the issue of public interest immunity in court proceedings. In *Uniform Evidence Law* (ALRC 102), the ALRC found that the procedures for invoking s 130 in court worked well.[117] The Report noted that the *National Security Information (Criminal and Civil Proceedings) Act* may replace the use of s 130 in a number of proceedings, although not all claims of public interest immunity involve matters of national security.

1.118 Given that the ALRC has recently made recommendations in regard to these issues, it is not proposed to revisit them in this Inquiry.

Options for reform

1.119 The ALRC is interested in hearing about whether the existing secrecy provisions reflect the value of protecting government information in an appropriate way and punish breaches accordingly. At the outset of this Inquiry it is instructive to ask broad questions to elicit responses that might assist the ALRC in undertaking the next stages of the consultative processes. To this end the ALRC is assessing whether the focus of this Inquiry should be placed on developing recommendations for:

- a new criminal offence of general application to the disclosure of Commonwealth information;
- the amendment and consolidation of existing Commonwealth secrecy laws;
- the repeal of unnecessary or unjustifiable Commonwealth secrecy laws;
- guidance on whether it is appropriate to introduce or retain a secrecy provision in federal legislation; or
- model secrecy provisions to assist in drafting future Commonwealth secrecy laws.

---

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

116 Protection of whistleblowers is discussed further in Chapter 4. In July 2008, the Australian Government referred the issue of whistleblower protection in the Australian Government public sector to the House of Representatives Standing Committee on Legal and Constitutional Affairs. The Committee is due to report in February 2009.

117 Australian Law Reform Commission, *Uniform Evidence Law* (2005), [15.158].

1.120 In ALRC 98 it was recommended that a duty of secrecy should be imposed only in relation to information that genuinely requires protection. The ALRC also recommended that a clear distinction should be drawn between conduct that gives rise to administrative sanctions under the *Public Service Act 1999* (Cth) and conduct that gives rise to criminal sanctions, including those under s 70 of the *Crimes Act 1914* (Cth).

1.121 As a preliminary matter—and to set the scene for a closer examination of the various issues raised in this Inquiry—a number of questions are asked in relation to the overall direction of the reform that may be considered. If some form of secrecy law is considered necessary in relation to information that genuinely requires protection, then the challenge is to decide what is the most effective and appropriate way to achieve this. The elements of the various secrecy laws are considered in Chapter 3; exceptions and defences in Chapter 4; and the penalty provisions in Chapter 5.

1.122 The ALRC is interested in hearing about the best way to manage issues concerning protection of Commonwealth information. Indeed, an important preliminary—and fundamental—question is to ask whether there need to be secrecy laws, as such, at all? Is information that genuinely requires protection controlled effectively through general law obligations?

1.123 The Terms of Reference also ask the ALRC to have regard to the increased need to share information within and between governments and the private sector. The expansion of government and the extensive use of contractors have created a new context for a consideration of the operation, effectiveness, and appropriateness of secrecy laws. The ALRC is interested in hearing about the impact that secrecy provisions have in this context.

Question 1–1 In light of freedom of information laws and other modern moves towards greater openness and accountability on the one hand, and the current international security environment on the other, are secrecy laws still relevant and necessary? Is a statutory duty on Commonwealth officers not to disclose information necessary or desirable? Are general law obligations sufficient and appropriate ways by which the disclosure of Commonwealth information may be regulated?

Question 1–2 Do federal secrecy provisions inhibit unduly the sharing of information within and between law enforcement agencies, governments, and between governments and the private sector?

Organisation of this Issues Paper

1.124 This Issues Paper is divided into 7 chapters. This first chapter has considered the context for secrecy provisions, relevant definitions and the scope of the Terms of Reference for this Inquiry, and possible options for reform.

1.125 Chapter 2 provides a broad overview of secrecy provisions in Commonwealth legislation. Commencing with a brief examination of the history of government secrecy in Australia, the chapter then reviews the number and location of secrecy provisions in Commonwealth legislation today and outlines the different types of information that these provisions are designed to protect.

1.126 Chapter 3 provides an analysis of the elements of secrecy and confidentiality provisions in Commonwealth legislation. In particular, this chapter examines questions such as whose activity is regulated by Commonwealth secrecy provisions, and what kind of activity is regulated. In addition, the chapter examines issues of form and consistency; whether existing provisions are consistent with the *Australian Constitution*, and the extent to which such provisions should be limited to conduct that is likely to harm the public interest.

1.127 Chapter 4 examines the manner in which exceptions and defences are formulated in Commonwealth secrecy and confidentiality provisions. The chapter also asks questions about the exceptions or defences that should apply in future. Exceptions and defences in relation to otherwise unauthorised handling of Commonwealth information also may arise under public interest disclosure (or 'whistleblower') legislation. Issues concerning existing and possible future public interest disclosure legislation and its relationship with secrecy laws are discussed.

1.128 Chapter 5 provides an analysis of the different types of penalties that apply when a secrecy provision is breached and highlights inconsistencies in the nature and levels of penalty that apply. The chapter raises questions about the best ways in which a consistent approach to penalties can be achieved and the broader issue of what the consequences of breaching secrecy provisions should be, including when it is appropriate for criminal, civil or administrative penalties to apply. It asks what type and level of penalty should apply and whether civil penalties should have a greater role to play in addressing unlawful handling of Commonwealth information. The chapter also considers some issues concerning the drafting of secrecy offences, including the location of provisions imposing significant criminal penalties—or imposing duties, the breach of which attracts such penalties—and the lack of clarity about the potential consequences attaching to breach.

1.129 Chapter 6 focuses on relevant practices relating to the protection of Commonwealth information and discusses the strategies used by the Australian Government in this area. In particular, the chapter examines the manner in which breaches are handled and investigated, and the role of bodies tasked to oversee and

monitor the information-protection strategies of Australian Government agencies. Questions are posed about what improvements could be made in this regard.

1.130 Chapter 7 considers the relationship between Commonwealth secrecy laws and other Commonwealth laws that deal with handling of information. The chapter asks what changes, if any, need be made to these laws to ensure an appropriate balance between the protection of Commonwealth information and an open and accountable system of government, and the protection of individual privacy.

Process of reform

Advisory Committee

1.131 It is standard operating procedure for the ALRC to establish an expert Advisory Committee to assist with the development of its inquiries.[118] In this Inquiry, the Advisory Committee includes judges, heads and senior officers of Australian Government agencies, academics, senior lawyers, and an FOI consultant.

1.132 The Advisory Committee met for the first time on 30 October 2008, and will meet at least two more times during the course of the Inquiry to provide advice and assistance to the ALRC. The Advisory Committee has particular value in helping the ALRC to identify the key issues, as well as in providing quality assurance in the research and consultation effort. The Advisory Committee will also assist with the development of reform proposals as the Inquiry progresses. However, the ultimate responsibility for the Report and recommendations remains with the Commissioners of the ALRC.

Community consultation and participation

1.133 Under the terms of its constituting Act, the ALRC 'may inform itself in any way it thinks fit' for the purposes of reviewing or considering anything that is the subject of an inquiry.[119] One of the most important features of ALRC inquiries is the commitment to widespread community consultation.[120]

1.134 The nature and extent of this engagement is normally determined by the subject matter of the reference. Areas that are seen to be narrow and technical tend to be of interest mainly to experts. Some ALRC inquiries—such as those relating to children and the law, Aboriginal customary law, multiculturalism and the law, the protection of

---

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

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

120 B Opeskin, 'Engaging the Public: Community Participation in the Genetic Information Inquiry' (2002) 80 *Reform* 53.

human genetic information, and privacy—involve a significant level of interest and involvement from the general public and the media.

1.135 To date, consultations have been held with a number of government agencies, academics, judges and members of the legal profession.

1.136 The ALRC will also be conducting a national 'phone-in' early in February 2009. Such a consultation strategy was undertaken during the Privacy Inquiry and proved a valuable means of obtaining personal experiences, insights, ideas and concerns that complemented the other forms of consultation through submissions and face-to-face meetings.[121]

1.137 To facilitate public communication in relation to the Inquiry, the ALRC will also be developing a 'Talking Secrecy' website, again following upon the success of the 'Talking Privacy' website established in connection with the Privacy Inquiry.[122] The object of such websites is to create a 'talking space' in relation to each ALRC inquiry, to provide information about the inquiry in an accessible manner. The 'Talking Secrecy' website will include a discussion page to encourage interactive comments in relation to matters raised during the Inquiry.

Participating in the Inquiry

1.138 There are several ways in which those with an interest in this Inquiry may participate. First, individuals and organisations may express an interest in the Inquiry by contacting the ALRC or applying online at <www.alrc.gov.au>. Those who wish to be added to the ALRC's mailing list will receive press releases and a copy of consultation documents related to the Inquiry.

1.139 Secondly, individuals and organisations may make written submissions to the Inquiry, both after the release of the Issues Paper and again after the release of the Discussion Paper. There is no specified format for submissions. The Inquiry will gratefully accept anything from handwritten notes and emailed dot-points, to detailed commentary. Submissions can be made by contributing comments online at the ALRC's website. The ALRC also accepts confidential submissions. Details about making a submission can be found at the front of this Issues Paper.

1.140 The ALRC strongly urges interested parties, and especially key stakeholders, to make submissions *prior* to the publication of the Discussion Paper. Once the basic pattern of proposals is established it is more difficult for the Inquiry to alter course radically. Although it is possible for the Inquiry to abandon or substantially modify proposals for which there is little support, it is more difficult to publicise, and gauge support for, novel approaches suggested to us late in the consultation process.

---

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

122 Ibid, [1.92]–[1.93].

1.141 Finally, the ALRC maintains an active program of direct consultation with stakeholders and other interested parties. The ALRC is based in Sydney but, in recognition of the national character of the Commission, consultations will be conducted around Australia during the Inquiry. Any individual or organisation with an interest in meeting with the Inquiry in relation to matters raised in this Issues Paper is encouraged to contact the ALRC.

Timeframe for the Inquiry

1.142 The ALRC's standard operating procedure is to produce an Issues Paper and a Discussion Paper prior to producing the final report.

1.143 The **Issues Paper** is the first document produced in the course of this Inquiry, and is intended to identify the main issues relevant to the Inquiry, provide background information, and encourage informed community participation. The Issues Paper is intended to stimulate full and open discussion of the issues arising from the Terms of Reference. At this early stage, the Inquiry is genuinely open to all approaches.

1.144 The Issues Paper will be followed by the publication of a **Discussion Paper** in late May 2009. The Discussion Paper will contain a more detailed treatment of the issues, and will indicate the Inquiry's current thinking in the form of specific reform proposals. The ALRC will then seek further submissions and undertake a further round of national consultations in relation to these proposals. Both the Issues Paper and the Discussion Paper may be obtained free of charge in hard copy or on CD from the ALRC or may be downloaded free of charge from the ALRC's website <www.alrc.gov.au>.

1.145 The **Report**, containing the final recommendations, is due to be presented to the Attorney-General by 31 October 2009. Once tabled in Parliament, the Report becomes a public document.[123] An ALRC Report is not a self-executing document—the ALRC provides recommendations about the best way to proceed, but implementation is a matter for Government and others.[124]

1.146 In recent reports, the ALRC's approach to law reform has involved a mix of strategies, including legislation and subordinate regulations; official standards and codes of practice; industry and professional guidelines; education and training programs; and so on. Although the final Report will be presented to the Attorney-

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

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

General, it is likely that some of its recommendations will be directed to other government and non-government agencies.

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

In order to be considered for use in the Discussion Paper, submissions addressing the questions in this Issues Paper must reach the ALRC by **Thursday, 19 February 2009**. Details about how to make a submission are set out at the front of this publication.

2. Overview of Secrecy Provisions in Commonwealth Legislation

Contents

Introduction

2.1 This chapter provides a broad overview of secrecy provisions in Commonwealth legislation. It commences by briefly examining the history of government secrecy in Australia. It then discusses the number and location of secrecy provisions in Commonwealth legislation today, and outlines the different types of information that these provisions are designed to protect. It concludes by considering the form of secrecy provisions.

2.2 Chapters 3–5 examine secrecy provisions in greater detail. Chapter 3 considers the elements of Commonwealth secrecy provisions. Chapter 4 examines the exceptions and defences available to those who are alleged to have breached the provisions, and Chapter 5 discusses the type and range of penalties imposed by the provisions.

2.3 As noted in Chapter 1, secrecy provisions are only one way in which the flow of Commonwealth information is regulated. Other legislative regimes, such as those established by the *Freedom of Information Act 1982* (Cth), the *Privacy Act 1988* (Cth) and the *Archives Act 1983* (Cth), also regulate access to, and disclosure of, Commonwealth information. So too do the mechanisms for classifying information according to different levels of security under the *Australian Government Protective Security Manual* (PSM).[1] In addition, administrative schemes and processes have an impact on the way in which Commonwealth information is handled. The other ways in which the flow of Commonwealth information is regulated are discussed in Chapters 6 and 7.

Government and secrecy in Australia

2.4 The history of government secrecy in Australia has been 'curiously underexplored'.[2] However, as Professor Enid Campbell has explained, the notion that the activities of government should be secret was imported from the United Kingdom, where 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.[3]

2.5 Secrecy was long held to be essential to the operation of the Australian political system, which is modelled on the 'Westminster system' of government.[4] The traditions or conventions of the Westminster system often support the notion of official secrecy. For example, the doctrine of collective ministerial responsibility depends to a large extent on the secrecy of Cabinet deliberations and documents; while the traditional view that the public service should be neutral and anonymous precludes public comment on government actions or policies by public servants.[5]

2.6 For most of Australia's history, 'official secrecy has been the legislatively enforced norm'.[6] The first secrecy provision was introduced in the colony of Victoria in 1867.[7] This provision, which 'set the pattern for the various public services of Australia',[8] provided that:

---

1 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual* (2005).

2 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 2.

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

4 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 34–35.

5 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.

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

7 Ibid, 89.

8 Ibid, 89.

> 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.[9]

2.7 The first Commonwealth secrecy provisions were passed during the first session of the Australian Parliament in 1901.[10] Early secrecy provisions aimed to protect national security information.[11] However, as John McGinness notes,

> with the expansion of the Commonwealth's role after the mid-1940s in areas such as taxation, health, education, welfare, scientific research, industry assistance and regulation, secrecy provisions increased in number as a reflection of the increase in personal and commercially sensitive information collected by the government.[12]

2.8 The need for government secrecy was reinforced during World War II and the Cold War, both of which 'provided a setting where secrecy was linked to military strength'.[13] 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'.[14] In 1960, amendments were made to s 70 of the *Crimes Act 1914* (Cth)[15] which had the effect of strengthening the provision. These amendments were inspired in part by the anti-communist climate of the Cold War.[16] However, as Greg Terrill notes, s 70 was 'just one of many secrecy provisions inserted or strengthened in legislation after the war'.[17]

2.9 The increase in the size and roles of government in the period following World War II, combined with technological advances which increased the ability of the government to deal with large amounts of information, had a significant impact on the nature of the relationship between citizens and the government.[18] In turn, the approach to official secrecy began to change in the 1960s with the development of a new philosophical and practical approach to government known as 'open government'.[19] As Terrill notes:

---

9 This provision was found in reg 20 of the 1867 Regulations for Victoria's *Civil Service Act 1862*: Ibid, 9.

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

11 Ibid, 49.

12 Ibid, 49.

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

14 Ibid, 41

15 Section 70 of the *Crimes Act 1914* (Cth) is a general secrecy provision which is discussed further below and set out in full in Appendix 3.

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

17 Ibid, 45.

18 Ibid, 42–43.

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

> 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.[20]

2.10 'Freedom of information' laws were the response. At this time, there was a growing interest in freedom of information legislation in Australia following the introduction of such legislation in the United States. A number of speeches, papers and editorials in Australia in the late 1960s and early 1970s raised the profile of the concept of freedom of information and propelled the inclusion on the parliamentary agenda of legislation of this kind.[21]

2.11 In 1970, the then Leader of the Opposition, the Hon Gough Whitlam MP, stated that 'it is clear that after 20 years in government excessive secrecy has become commonplace in governmental decision making'.[22] Introduction of freedom of information legislation became an issue prior to 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]

2.12 The introduction of freedom of information legislation remained a political issue during the 1970s.[25] At this time, other approaches were also pursued to establish a more open system of public administration. For example, in the mid-1970s, the *Administrative Appeals Tribunal Act 1975* (Cth), the *Ombudsman Act 1976* (Cth) and the *Administrative Decisions (Judicial Review) Act 1977* (Cth) were passed. These Acts all establish mechanisms for enhancing the accountability of government departments and public servants. In 1982, the *Freedom of Information Act* was passed, embracing in a formal way the concept of open government.

2.13 The philosophy of open government conflicted diametrically with secrecy provisions, as the Senate Standing Committee on Legal and Constitutional Affairs

---

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

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

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

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

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

25 See, eg, Interdepartmental Committee on Proposed Freedom of Information Legislation, *Proposed Freedom of Information Legislation* (1974) Australian Government Attorney-General's Department; Interdepartmental Committee on Proposed Freedom of Information Legislation, *Policy Proposals for Freedom of Information Legislation: Report of Interdepartmental Committee* (1976) Australian Government Attorney-General's Department; Parliament of Australia—Senate Standing Committee on Constitutional and Legal Affairs, *Freedom of Information: Report by the Senate Standing Committee on Constitutional and Legal Affairs on the Freedom of Information Bill 1978, and Aspects of the Archives Bill 1978* (1979).

noted when commenting on the Freedom of Information Bill 1978 (Cth).[26] The Committee also criticised what it described as 'a fashionable contemporary drafting practice'

> to insert in every new statute a standard provision making it an offence for an official governed by the statute to disclose without authorisation any information of which he has gained knowledge officially.[27]

2.14 Accordingly, the unresolved issue of the proper role of secrecy provisions was acknowledged from the outset of the freedom of information era in Australia. The conflict between the secrecy required of Commonwealth officers and open government—as a philosophy of government—remains today. In fact, it has been noted that:

> 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.[28]

Number and location of Commonwealth secrecy provisions

2.15 At the outset of the Inquiry, the ALRC commenced a 'mapping exercise', analysing provisions in Commonwealth legislation that impose secrecy or confidentiality obligations on individuals or bodies in respect of the handling of Commonwealth information. This mapping exercise is ongoing and, while time consuming, will facilitate the formulation of sound, evidence-based proposals and recommendations for law reform in this area.

2.16 To date, the ALRC has identified 370 distinct secrecy provisions. These provisions are scattered throughout 166 pieces of primary and subordinate legislation and are set out in Appendix 2. The list in Appendix 2 does not include provisions which only clarify or otherwise inform the operation of a secrecy provision, such as provisions which set out the circumstances in which the handling of Commonwealth information will not breach a secrecy provision (exception provisions). The ALRC is interested in hearing if there are other secrecy provisions that are not included in Appendix 2.

2.17 The majority of the secrecy provisions identified by the ALRC to date establish one or more criminal offences. Most of these are indictable offences—that is, offences punishable by imprisonment for a period exceeding 12 months.[29] The remainder are

---

26 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.

27 Ibid, 233.

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

29 *Crimes Act 1914* (Cth) s 4G.

summary offences—that is, offences which are not punishable by imprisonment, or are punishable by imprisonment for a period not exceeding 12 months.[30] The ALRC has identified only one civil penalty provision in its mapping exercise.[31]

2.18 A relatively small number of provisions identified by the ALRC simply set out rules for the handling of Commonwealth information.[32] The existence of such a provision could be used to support the argument that a Commonwealth officer had a duty not to disclose information in a prosecution for an alleged breach of ss 70 or 79(3) of the *Crimes Act*. However, the consequences of a breach of such a provision are not always clear.[33]

2.19 A breach of a secrecy provision may also result in the imposition of an administrative penalty, such as dismissal from employment. Administrative and other penalties for breaches of secrecy provisions are discussed in Chapter 5.

Types of secrecy provisions

2.20 As noted above, there are hundreds of secrecy provisions located in different pieces of primary and subordinate Commonwealth legislation. These provisions have been introduced at various times over the past 100 years and, as such, differ widely in their language and scope.

2.21 In *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the ALRC recognised that 'a certain amount of flexibility across the range of Commonwealth secrecy provisions is acceptable', but expressed concern about the lack of consistency in the fundamental principles underpinning the provisions.[34]

2.22 In this chapter, the ALRC has used the language of the provisions identified to date to divide them into categories. These categories are not mutually exclusive and at times overlap. For example, a secrecy provision that protects 'any information acquired in the course of official duties' could in fact protect 'information about the affairs of person', 'confidential information', or 'law enforcement information'. Similarly, a provision that protects 'information about the affairs of a person' could protect 'taxation information' if it is contained in a piece of taxation legislation.

2.23 In 1991, the Review of the Commonwealth Criminal Law, conducted by a committee chaired by Sir Harry Gibbs (the Gibbs Committee), recommended that the 'catch-all' provisions of ss 70 and 79(3) of the *Crimes Act* be repealed and replaced

---

30 Ibid s 4H.
31 *Workplace Relations Act 1996* (Cth) sch 1, s 276. Civil penalty provisions are discussed in Ch 5.
32 See, eg, *Archives Act 1983* (Cth) s 30A.
33 The consequences of breaching a secrecy provision are discussed in Ch 5.
34 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), [5.118].

with provisions that impose criminal sanctions for the disclosure of certain types of information. The Committee recommended that these types of information include:

- information relating to intelligence and security services, defence and foreign relations;
- information obtained in confidence from, or entrusted in confidence to, other governments or international organisations;
- information the disclosure of which would be likely to result in the commission of an offence; facilitate an escape from legal custody or the doing of an act prejudicial to the safekeeping of persons in legal custody; or impede the prevention or detection of offences or the apprehension or prosecution of suspected offenders.[35]

2.24 The Gibbs Committee concluded that it was also necessary to prove that the disclosure caused damage in certain circumstances. The Committee's recommendations are discussed further in Chapter 3.

2.25 The ALRC has categorised secrecy provisions according to the information that each provision seeks to protect. In doing this, the ALRC aims to facilitate analysis of the provisions and generate discussion on some of the fundamental questions arising in this Inquiry—namely, what type or types of Commonwealth information should be protected by secrecy provisions, and in what circumstances?

General secrecy provisions

2.26 The next section of this chapter examines general secrecy provisions that protect any Commonwealth information. These include provisions contained in the *Crimes Act*, as well as provisions contained in other Commonwealth Acts.

Provisions in the *Crimes Act 1914* (Cth)

2.27 The Terms of Reference direct the ALRC to consider whether there is a need to consolidate and modernise relevant provisions currently in the *Crimes Act* and other Commonwealth legislation for inclusion in the *Criminal Code 1995* (Cth).

2.28 The *Criminal Code* was introduced as a schedule to the *Criminal Code Act 1995* (Cth), and entered into force on 1 January 1997. The Australian Government intends the *Criminal Code* to be the principal piece of federal legislation containing serious criminal offences. Substantive criminal provisions in other, older pieces of

35 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.50].

law, such as the *Crimes Act*, will progressively be reviewed, and either 'modernised' and 'migrated' to the *Criminal Code*, or repealed. Ultimately, the *Crimes Act* will be left covering matters of police powers (such as arrest, detention, search and seizure, forensic procedures) and criminal procedure.

2.29 Underlying this process is the desire to keep the Commonwealth criminal statute book 'fresh'—utilising modern drafting techniques, providing greater uniformity of language and concepts, and ensuring that the law keeps abreast of contemporary circumstances, attitudes and concerns.[36]

2.30 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, while s 79 deals with the disclosure of 'official secrets'. 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'.[37]

2.31 In some circumstances, the unauthorised disclosure of Commonwealth information may amount to an offence under a general secrecy provision in the *Crimes Act* as well as an offence under a secrecy provision in another piece of Commonwealth legislation. In these situations, an alleged offender can be prosecuted under either law.[38] However, when determining the charges to be laid or proceeded with, the Commonwealth Director of Public Prosecution's *Prosecution Policy of the Commonwealth* states that the provisions of a specific Act should be relied upon rather than the general provisions of the *Crimes Act*, unless to do so 'would not adequately reflect the nature of the criminal conduct disclosed by the evidence'.[39]

2.32 Each of the general secrecy provisions in the *Crimes Act* will be considered in turn. As they are central to this Inquiry, both provisions are included in Appendix 3.

Section 70—Disclosure of information by Commonwealth officers

2.33 Section 70 of the *Crimes Act* is a general prohibition against the unauthorised disclosure of official information by Commonwealth officers. Section 70 is the only provision remaining in Part VI of the *Crimes Act*, which is entitled 'Offences by and

---

36 The development of the *Criminal Code* was considered in detail in Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Ch 1.

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

38 *Crimes Act 1914* (Cth) s 4C.

39 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <www.cdpp.gov.au/Publications/ProsecutionPolicy/> at 26 August 2008, [2.22].

against Public Officers'.[40] A version of s 70 was included in the original *Crimes Act* in 1914, and was based on a provision of the *Criminal Code 1899* (Qld).[41]

2.34 This original version of s 70 was repealed and replaced in 1960.[42] The new s 70 extended the prohibition on the unauthorised disclosure of information by Commonwealth officers to *former* Commonwealth officers. While minor amendments have been made to s 70 on three occasions since 1960,[43] the substance of the provision has not changed since that time.

2.35 Currently, s 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.
>
> Penalty: Imprisonment for 2 years.

2.36 A 'Commonwealth officer' is defined as 'a person holding office under, or employed by, the Commonwealth'.[44] Further, for the purposes of s 70, a Commonwealth officer also includes a person who performs services for the Commonwealth, a public authority under the Commonwealth, or a Territory; and a person who is employed by or performs services for the Australian Postal Corporation.[45] In addition, a Commonwealth officer includes an officer or employee of the Australian Security Intelligence Organisation (ASIO)[46] and a staff member of the Australian Secret Intelligence Service (ASIS).[47]

---

40 The other offence provisions in Part 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 1995*.

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

42 *Crimes Act 1960* (Cth).

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

44 *Crimes Act 1914* (Cth) s 3.

45 Ibid s 3.

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

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

2.37 A critical point in the analysis of s 70 is that the section does not of itself give rise to a duty not to disclose information. Instead, the source of such a duty must be found elsewhere. For example, the source of the duty may be the common law duty of an employee to serve his or her employer in good faith and fidelity; an equitable duty of confidence;[48] or a specific legislative provision giving rise to a duty not to disclose official information.[49] However, the word 'duty' in this section is somewhat ambiguous. It has been argued, for example, that the word refers to a legal duty, as opposed to a contractual or moral duty,[50] although the source of this legal duty is not always clear.

> Whether the duty may be found in the express terms and conditions in the person's contract of employment, or in the absence of such a term may be implied, is unclear. It is submitted that 'duty' in s 70 refers to a legal duty, that is, one clearly imposed by some other statutory provision or rule of law … This poses difficulties in successfully prosecuting persons who are not employed by the Commonwealth, such as contractors, consultants and State officers, notwithstanding that such persons perform services for or on behalf of the Commonwealth, thus falling within the definition of 'Commonwealth officer' in s 3 of the *Crimes Act*.[51]

2.38 Other aspects of s 70 have also been criticised for their ambiguity. It has been argued, for example, that the provision provides no guidance on the circumstances in which a disclosure will be 'authorised',[52] or on the meaning of the words 'fact' and 'document'.[53]

2.39 Section 70 is broad in its operation. It applies to any information, regardless of its nature or the effect of its disclosure.[54] As far back as the original debates in 1914, before the passage of the *Crimes Act*, it was described as 'a pretty wide provision',[55] and since its introduction numerous bodies and government inquiries have recommended that it be reformed. For example:

- In 1979, the Senate Standing Committee on Constitutional and Legal Affairs urged the Australian Government to reconsider s 70 in light of its report on the Freedom of Information Bill 1978.[56] The Committee expressed the view that it was 'implausible to enact a presumption of openness while leaving untouched

---

48 The common law duty of fidelity and loyalty and the equitable duty of confidence are discussed in Ch 1.

49 See, eg, *R v Goreng Goreng* [2008] ACTSC 74, [8]; *Johnston v Director of Public Prosecutions (Cth)* (1989) 90 ACTR 7, 9–10.

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

51 Ibid, 258–259. The definition of a 'Commonwealth officer' is discussed below.

52 Ibid, 260.

53 Ibid, 260.

54 *Commissioner of Taxation v Swiss Aluminium Australia Ltd* (1986) 10 FCR 321, 325.

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

56 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].

provisions like section 70 that provide the legal foundation for the system of discretionary secrecy that presently exists'.[57]

- In 1983, the Human Rights Commission noted that s 70 could operate in a manner inconsistent with art 19 of the *International Covenant on Civil and Political Rights* (ICCPR), which deals with the right to freedom of expression.[58] The Commission noted that s 70 was broad, in that it applied to any information regardless of its nature, and recommended that it be amended so that it only protected the kinds of information in respect of which restrictions may be imposed under the ICCPR.[59]

- In 1991, the Gibbs Committee recommended that s 70 of the *Crimes Act* be repealed and replaced by provisions prohibiting the disclosure of certain types of information (outlined above).[60]

- 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.[61]

2.40 There have been several successful prosecutions for breaches of s 70. For example, the provision has been used to prosecute:

- a member of the Australian Federal Police (AFP) for disclosing information held in AFP files to a private business associate;[62]

- an officer of the Australian Taxation Office for providing documents containing summaries of taxpayers and tax agents to a private business associate;[63]

- an officer of the Australian Customs Service for providing reports about security at Sydney Kingsford Smith Airport to journalists;[64] and

---

57 Ibid, [21.24].
58 Human Rights Commission, *Review of the Crimes Act 1914 and Other Crimes Legislation of the Commonwealth* (1983), [26].
59 Ibid, [26], [54(8)].
60 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.5], Rec 35.1.
61 Australian Parliament—Senate Select Committee on Public Interest Whistleblowing, *In the Public Interest* (1994), [9.53].
62 *Johnston v Director of Public Prosecutions (Cth)* (1989) 90 ACTR 7.
63 *R v Petroulias (No 36)* [2008] NSWSC 626 .
64 *R v Kessing* [2007] NSWDC 138.

- an officer of the Office of Indigenous Policy Coordination for disclosing information relating to the then draft *Declaration on the Rights of Indigenous Peoples* to her daughter, and information relating to Commonwealth Indigenous policy to a member of the Mutitjulu community.[65]

2.41 The ALRC is interested in views about whether a general offence provision such as s 70 remains desirable and appropriate today and, if so, where it should be located. In Chapter 4 the ALRC asks what exceptions or defences should be incorporated into any such general criminal offence provision.[66] The ALRC is also interested in views on how any such provision should be framed, and whether it is appropriate for it to rely on a duty not to disclose Commonwealth information that arises separately, for example, under the common law, in equity or under other legislative provisions.

Question 2–1 Should the unauthorised handling of Commonwealth information remain subject to a general criminal offence? If so, should s 70 of the *Crimes Act 1914* (Cth) be repealed and replaced by an updated offence in the *Criminal Code* (Cth)?

Question 2–2 If it is appropriate to retain a general criminal offence for unauthorised handling of Commonwealth information, how should that provision be framed? Is it appropriate for such a provision to rely on a duty arising separately under the general law or under other legislative provisions?

Section 79—Unauthorised communication of official secrets

2.42 Section 79 of the *Crimes Act* deals with the disclosure of official secrets.[67] It was introduced in the original Act, and was based on provisions in the *Official Secrets Act 1911* (UK).[68]

2.43 Section 79 is concerned, to some extent, with espionage and espionage related matters. The Criminal Code Amendment (Espionage and Related Offences) Bill 2001, discussed below, was intended, among other things, to repeal and replace s 79 of the *Crimes Act* with updated provisions in the *Criminal Code*. Following some controversy, however, the provisions intended to replace s 79 were removed from the Bill.[69]

---

65 *R v Goreng Goreng* [2008] ACTSC 74.
66 Question 4–1.
67 Section 79 is set out in full in Appendix 3.
68 Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney General), 265.
69 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Provisions of the Criminal Code Amendment (Espionage and Related Offences) Bill 2002* (2002), 1.

2.44 Section 79 creates a number of offences relating to the use and disclosure of 'official information'—that is, a sketch, plan, photograph, model, cipher, note, document, article or information obtained:

- in contravention of Part VII of the *Crimes Act* or s 91.1 of the *Criminal Code*;
- from a Commonwealth officer or a person holding office under the Queen, where the person obtaining it has a duty to treat it as secret;
- by a person by virtue of his or her position as, among other things, a Commonwealth officer, where he or she has a duty to treat the information as secret; or
- by a person who knows, or ought to know, that information relating to a prohibited place or anything in a prohibited place[70] should not be communicated to a person not authorised to receive it.[71]

2.45 In summary, s 79(2) makes it an offence, punishable by seven years imprisonment, to communicate or retain official information with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions. Section 79(3) makes it an offence, punishable by two years imprisonment, to communicate official information in an unauthorised manner, while ss 79(4)–(6) create offences relating to the unauthorised retention and receipt of official information.

2.46 Section 79(7) provides that, in a prosecution under s 79(2), the circumstances of the case, or evidence of the accused's conduct or character, may be used to prove the accused had an intention to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions. Section 79(8) gives a magistrate or judge the discretion to exclude evidence about the circumstances of the case, the accused's conduct or the accused's character in certain circumstances; while s 79(9) outlines the directions that a trial judge must give a jury if evidence of this kind is admitted at trial. Section 79(10) enables a person charged with an offence against s 79(2) to be found guilty of an offence against s 79(3), and a person charged with an offence against s 79(5) to be found guilty of an offence against s 79(6).

2.47 In common with s 70, s 79 applies to *all* information, regardless of its nature or the effect of its disclosure. It applies whether or not the alleged offender was aware that he or she had a duty not to disclose information.[72] In addition, as with s 70, the duty to treat information as secret is not established by s 79 and must be found elsewhere.

---

70 'Prohibited place' is defined in s 80 of the *Crimes Act 1914* (Cth).
71 Ibid s 79(1).
72 *Grant v Headland* (1977) 17 ACTR 29, 31.

2.48 There are several ambiguities in the scope and operation of s 79. For example, although s 79 is not limited in its scope to current and former Commonwealth officers, the source and nature of the duty of others to treat information as secret is unclear.[73] Further, the provision provides no guidance on the circumstances in which a disclosure of official information will be 'authorised', or when it is in 'the interest of the Commonwealth or part of the Queen's dominions' to communicate it. There is little judicial guidance on s 79 as there have been very few prosecutions of offences under the provision.[74]

2.49 Section 79 has been criticised by several review bodies. For example:

- In 1983, the Human Rights Commission noted that s 79(7) eroded the presumption of innocence in art 14.2 of the ICCPR, and recommended that it be amended to bring it into line with the ICCPR.[75]

- In 1991, the Gibbs Committee recommended that s 79(3) of the *Crimes Act* be repealed and replaced by provisions prohibiting the disclosure of certain types of information (outlined above).[76]

- In 2004, the ALRC recommended that the Australian Government review s 79 to clarify and modernise the language and intent of the provision and to ensure that an appropriate public policy balance is found across the range of offences created by the provision.[77]

Overlap between the Crimes Act and Criminal Code

2.50 There is some overlap between s 79 of the *Crimes Act,* s 70 of the *Crimes Act* and s 91.1 of the *Criminal Code.* Section 79(3) of the *Crimes Act*, which deals with the unauthorised communication of official information, overlaps to some extent with s 70; while some of the offences under s 79 that require an act to be committed with the intention of prejudicing the security or defence of the Commonwealth overlap with the espionage offences in s 91.1 of the *Criminal Code*.

2.51 Section 91.1 of the *Criminal Code* contains the major offences relating to espionage. The text of s 91.1 is set out in Appendix 3. In summary, s 91.1(1) makes it an offence to communicate information about the security or defence of the Commonwealth, or information about the security or defence of another country that

---

73 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 264.

74 *R v Lappas* (2003) 152 ACTR 7*; Grant v Headland* (1977) 17 ACTR 29.

75 Human Rights Commission, *Review of the Crimes Act 1914 and Other Crimes Legislation of the Commonwealth* (1983), [28], [54(10)].

76 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), [31.5], Rec 35.1.

77 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–4.

was obtained from the Commonwealth, to another country or foreign organisation with the intention of prejudicing the security or defence of the Commonwealth. Section 91.1(2) makes it an offence to communicate such information to another country or foreign organisation without lawful authority, with the intention of giving an advantage to another country's security or defence.

2.52 Section 91.1(3) makes it an offence to make, obtain or copy a record of such information with the intention of delivering it to another country or foreign organisation in order to prejudice the security or defence of Australia; while s 91.1(4) makes it an offence to make, obtain or copy a record of such information with the intention of delivering it to another country or foreign organisation, without lawful authority, in order to give an advantage to another country's security or defence. All of the offences in s 91.1 carry a penalty of imprisonment for 25 years.

2.53 The offences in s 91.1 were moved from the *Crimes Act* to the *Criminal Code* as part of the reforms included in the *Criminal Code Amendment (Espionage and Related Offences) Act 2002* (Cth).[78] The new *Criminal Code* updated the terminology and concepts contained in the previous *Crimes Act* provisions by, for example, replacing references to 'plans, photographs, models, ciphers, notes, documents and articles' with the broader terms 'information' and 'records'.

2.54 The relationship between s 79 of the *Crimes Act* and s 91.1 of the *Criminal Code* is unclear. This is particularly the case in relation to ss 79(2) and 79(5)—which attract the highest maximum penalty under s 79 of seven years imprisonment.

2.55 It is an offence under s 79(2)(a) of the *Crimes Act* to communicate official information with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions.[79] This provision overlaps with s 91.1(1) of the *Criminal Code*.

2.56 Section 79(5) of the *Crimes Act* makes it an offence for a person to receive an official secret knowing, or having reasonable grounds to believe, that it is communicated to him or her in contravention of s 91.1 of the *Criminal Code* or s 79(2) of the *Crimes Act*, unless he or she can prove that the communication was contrary to his or her desire. This offence does not require an intention to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions, but it carries the same penalty as s 79(2)—seven years imprisonment.

---

78 Espionage offences were previously in pt VII of the *Crimes Act 1914* (Cth). Section 78 of the *Crimes Act* was repealed and re-enacted, albeit in somewhat different terms and with significantly higher penalties, as s 91.1 of the *Criminal Code* (Cth).

79 References to the 'Queen's dominions' were removed in the new *Criminal Code* provisions, but remain in some *Crimes Act* provisions.

2.57 Given the overlap between the provisions in the *Criminal Code* and the *Crimes Act*, it is arguable that s 79(2)(a) could be repealed and not replaced. However, some of the offences in s 79 are not replicated exactly in s 91.1 of the *Criminal Code.* These include some offences involving an intention to prejudice the security or defence of the Commonwealth (namely, offences relating to the retention and disposal of official information),[80] and some offences relating to the communication, retention, disposal and care of official secrets that do not require an intention to prejudice the security or defence of the Commonwealth.[81]

2.58 Given the overlap between s 70 of the *Crimes Act*, s 79 of the *Crimes Act* and s 91.1 of the *Criminal Code Act*, the ALRC is interested in receiving stakeholder views on whether there is a need to retain any of the offences currently set out in s 79 and, if so, how those offences should be framed.

Question 2–3 Given the overlap between s 70 of the *Crimes Act 1914* (Cth), s 79 of the *Crimes Act* and s 91.1 of the *Criminal Code* (Cth), should any of the offences currently in s 79 be retained and replaced by updated offences in the *Criminal Code*? If so, how should those offences be framed?

Provisions that protect information obtained in the course of official duties

2.59 A number of Commonwealth secrecy provisions aim to prevent the unauthorised disclosure of any information obtained by a person during the course of his or her employment.[82] Generally, these provisions prohibit the disclosure of information obtained by a person carrying out, performing or exercising any of the person's duties, functions or powers under: (a) the Act in which the provision is located; (b) a particular part of the Act in which the provision is located; (c) regulations made under the Act in which the provision is located; or (d) another Act.

2.60 Secrecy provisions in this category protect any information obtained by a government official in the course of his or her employment, regardless of its nature or the effect of its disclosure. It is even arguable that they prohibit the disclosure of information that is already in the public domain.

2.61 Australian Public Service (APS) employees have a general duty not to disclose official information. Section 13 of the *Public Service Act 1999* (Cth) sets out the APS

---

80 *Crimes Act 1914* (Cth) s 79(2)(b), (c).

81 Ibid s 79(3), (4), (6).

82 See, eg, *Australian Crime Commission Act 2002* (Cth) s 51(2); *Auditor-General Act 1997* (Cth) s 36; *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); *Trade Practices Act 1974* (Cth) s 95ZP(1).

Code of Conduct which requires an employee, for example, to behave honestly and with integrity in the course of his or her employment,[83] and to maintain appropriate confidentiality about dealings the employee has with any minister or minister's member of staff.[84] 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—pursuant to which, reg 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.[85]

2.62 The effect of provisions that protect any information obtained in the course of official duties on the flow of Commonwealth information depends to a large extent on the breadth of their exceptions. For example, a person regulated by s 95ZP of the *Trade Practices Act 1974* (Cth) must not disclose information except in the course of performing or exercising functions, powers or duties under or in relation to the *Trade Practices Act*. In contrast, a person regulated by s 16 of the *Customs Administration Act 1985* (Cth) may record or disclose information in a range of identified circumstances, including when the recording or disclosure has been authorised by the Chief Executive Officer, or when there are reasonable grounds to believe that it is necessary to avert or reduce a serious or imminent threat to the health or life of a person or persons.[86] Exceptions and defences to secrecy provisions are discussed in Chapter 4.

Provisions that protect specific types of Commonwealth information

2.63 A great number of secrecy provisions prohibit the unauthorised handling of specific types of Commonwealth information, such as information about the affairs of a person or taxation information, although the current policy expressly discourages this approach where general provisions would otherwise apply. The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that:

> The *Criminal Code* and *Crimes Act* … contain offences of general relevance to Commonwealth administration. These provisions should not be replicated.
>
> Broadly framed provisions of general application were placed in the Criminal Code to avoid the technical distinctions, loopholes, additional prosecution difficulty and

---

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

84 Ibid s 13(6).

85 Reg 2.1 was amended in 2006, following the decision in *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119. The issues that arose for consideration in that case are discussed further in Ch 3. The text of reg 2.1 of the *Public Service Regulations* is set out in Appendix 3.

86 *Customs Administration Act 1985* (Cth) s 16(3)–(10).

> appearance of incoherence associated with having numerous slightly different provisions to similar effect across Commonwealth law. There are also some provisions concerning offences in the *Crimes Act*. It is intended that these will be transferred to the *Criminal Code* in due course.
>
> Where a relevant *Criminal Code* or *Crimes Act* provision applies, separate provision should not be made in another Act.[87]

2.64 In contrast, however, McGinness has suggested that:

> General secrecy provisions need to be replaced by specific provisions which introduce certainty and consistency to the regulation of unauthorised public disclosure. The challenge in any reform of secrecy provisions is to identify and define those categories of information which require the special protection of the criminal law.[88]

Information about the affairs of a person

2.65 A significant proportion of Commonwealth secrecy provisions aim to prevent the unauthorised disclosure of information about individuals held by government agencies.[89]

2.66 The majority of these provisions establish one or more criminal offences. However, a small number simply provide that a person has a duty not to publish or communicate information about another person.[90] These could be used to establish that a Commonwealth officer had a duty not to disclose information in a prosecution of an alleged breach of ss 70 or 79(3) of the *Crimes Act*.

2.67 Generally, these provisions prohibit government officials from recording or disclosing information about other people acquired by virtue of their office, subject to certain exceptions. Some also prohibit obtaining unauthorised access to,[91] soliciting the disclosure of,[92] or offering to supply,[93] information about people held by certain government agencies. A small number also prohibit the secondary or subsequent disclosure of the information.[94] For example, s 86–5 of the *Aged Care Act 1997* (Cth) provides that a person is guilty of an offence if he or she records, discloses or uses

---

87 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 16.

88 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 61.

89 The word 'person' in a secrecy provision includes a body politic or corporate as well as an individual: *Acts Interpretation Act 1901* (Cth) s 22.

90 *Building and Construction Industry Improvement Act 2005* (Cth) s 66; *Census and Statistics Act 1905* (Cth) s 12; *Export Finance and Insurance Corporation Act 1991* (Cth) s 87(4).

91 *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 164; *Social Security (Administration) Act 1999* (Cth) s 203.

92 *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 165; *Social Security (Administration) Act 1999* (Cth) s 205.

93 *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 166; *Social Security (Administration) Act 1999 (Cth)* s 206.

94 *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(4); *Child Support (Assessment) Act 1989* (Cth) s 150AA; *Child Support (Registration and Collection) Act 1988* (Cth) s 58.

information provided under ss 86–3 or 86–4 of the Act for a purpose other than that for which it was provided.

2.68 Some secrecy provisions that protect information of this type use the term 'personal information'.[95] This is the term used in the *Privacy Act* and the *Freedom of Information Act*, two Acts that also regulate the disclosure of information about persons held by Australian Government agencies. Others refer to information 'about a person',[96] or 'concerning another person',[97] while a small number refer to 'identifying information',[98] or information that would enable people generally to 'work out the identity of the individual to whom the information relates'.[99] The majority, however, refer to information about the 'affairs' of another person.

2.69 The relationship between secrecy provisions and the *Privacy Act* is discussed in Chapter 7, where the ALRC asks whether secrecy provisions should regulate personal information and, if so, whether they should refer to, or use the terminology of, the *Privacy Act*.[100]

Taxation information

2.70 A number of secrecy provisions aim to prevent the unauthorised disclosure of 'taxation information'. For the purposes of this discussion, 'taxation information' is defined as information provided by a taxpayer to a person or an agency pursuant to a legislative requirement contained in taxation legislation.

2.71 Secrecy provisions have long been used to protect the unauthorised disclosure of taxation information and the Australian Taxation Office has a strong culture of security consciousness about taxpayer information.[101] For example, s 16 of the *Income Tax Assessment Act 1936* (Cth) has been present in the Act since its introduction. The justification for the protection of taxation information is that it encourages voluntary

---

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

96 See, eg, *Superannuation Contributions Tax (Assessment and Collection) Act 1997* (Cth) s 32(1), (2); *Superannuation Contributions Tax (Members of Constitutionally Protected Superannuation Funds) Assessment and Collection Act 1997* (Cth) s 28(1),(2); *Termination Payments (Assessment and Collection) Act 1997* (Cth) s 23(1), (2); *Superannuation Guarantee (Administration) Act 1992* (Cth) s 45(1), (2).

97 *Australian Institute of Health and Welfare Act 1987* (Cth) s 29.

98 See, eg, *Australian Citizenship Act 2007* (Cth) ss 42–43; *Migration Act 1958* (Cth) s 336E.

99 *Workplace Relations Act 1996* (Cth) ss 163C(1)(b), 166T(1)(b).

100 Question 7–4. The relationship between the *Privacy Act 1988* (Cth) and secrecy provisions was also discussed in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), Ch 15.

101 This was noted by an independent consultant engaged by the Australian Taxation Office in 2008 to review its information security practices: Australian Taxation Office, *Annual Report 2007–08* (2008), [1.1].

compliance with taxation legislation.[102] It has been noted that 'compliance with tax laws could be adversely affected if taxpayers thought their personal information could be disclosed easily'.[103] Secrecy provisions protecting taxation information almost always criminalise the unauthorised disclosure of the information.

2.72 Some of the secrecy provisions that protect taxation information specifically refer to the type of information protected. For example, s 8WB(1)(c) of the *Taxation Administration Act 1953* (Cth) prohibits the disclosure of a 'tax file number'. However, most of the provisions prohibit the disclosure of information about a person that was disclosed or obtained under a piece of taxation legislation.[104] Some provisions also include the additional requirement that the information was obtained in the course of official employment.[105]

2.73 Further, a number of secrecy provisions that protect taxation information deal with the subsequent disclosure of the information. For example, s 3EA(2) of the *Taxation Administration Act 1953* (Cth) makes it an offence for an ASIO officer to disclose taxation information that he or she has obtained from the Commissioner of Taxation pursuant to s 3EA(1) of the Act.

2.74 In 2006, the Treasury undertook a review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review).[106] In its discussion paper, the Treasury noted that taxation secrecy provisions are located in numerous different Acts, differ in their language and scope, and have inconsistent penalties.[107] Further, it noted that some provisions merely duplicate provisions located in other Acts.[108]

2.75 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, Australian Business Number and Tax File Number disclosures) be standardised and consolidated into a single piece of legislation.[109] It proposed that any new provision or provisions dealing with the disclosure of taxpayer information should, among other things, clearly describe what information is protected and by whom.[110]

---

102 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 1.
103 Ibid, [1.1].
104 See, eg, *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth); *Child Support (Assessment) Act 1989* (Cth) s 150(2); *Inspector-General of Taxation Act 2003* (Cth) (Cth) s 37(2).
105 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30(2); *Petroleum Resource Rent Tax Assessment Act 1987* (Cth) s17(3); *Excise Act 1901* (Cth) s 159(2); *Higher Education Funding Act 1988* (Cth) s 78(4); *Income Tax Assessment Act 1936* (Cth) s 16(2).
106 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006).
107 Ibid, [2.1].
108 Ibid, [2.1].
109 Ibid, [2.3].
110 Ibid, [2.3], [3.2]. To date, these proposals have not been implemented.

Census and statistical information

2.76 The Australian Bureau of Statistics (ABS) conducts a census of population and housing every five years in accordance with the *Census and Statistics Act 1905* (Cth).[111] The census aims 'to accurately measure the number of people in Australia on Census Night, their key characteristics, and the dwellings in which they live', and

> to provide timely, high quality and relevant data for small geographic areas and small population groups, to complement the rich but broad level data provided by ABS surveys.[112]

2.77 The census is regarded as the most important source of statistical information in Australia. The information from the census is used to produce statistical data for use by governments, as well as academics, businesses and private individuals. Section 19(1) of the *Census and Statistics Act* makes it an offence for any past or present officer of the ABS to disclose any information given under the Act. Section 19A of the Act provides that an officer of the ABS must not be required to disclose census information to an agency for 99 years following a census, unless the disclosure is in accordance with the Act.

2.78 Census information may be transferred to the National Archives of Australia in certain circumstances.[113] A record containing census information is not available for public access for 99 years.[114] Section 30A of the *Archives Act 1983* (Cth) prohibits an Archives officer from disclosing census information before the information is available for public access. This is not an offence provision, but it does create a duty not to disclose information that could be used to support a prosecution of a breach of s 70 of the *Crimes Act*.

2.79 The ABS also produces statistics on a wide range of social and economic matters. Several provisions of the *Census and Statistics Act* deal with the disclosure of information given under the Act. As noted above, s 19(1) makes it an offence for any past or present officer of the ABS to disclose any information given under the Act, otherwise than in accordance with a ministerial determination under s 13(1),[115] or for the purposes of the Act. Section 19(2) makes it an offence for a person to whom information has been disclosed pursuant to a determination under s 13(1) to fail to comply with an undertaking given in relation to the information.

2.80 In addition, s 12 of the Act provides that the results of any analysis of statistical information shall not be published in a manner that is likely to enable the identification

---

111 *Census and Statistics Act 1905* (Cth) s 8.
112 Australian Bureau of Statistics, *How Australia Takes a Census*, 2903.0 (2006), vii.
113 *Census and Statistics Act 1905* (Cth) s 8A.
114 Ibid s 22B.
115 Under s 13(1) the Minister may, by legislative instrument, make determinations providing for and in relation to the disclosure of information (with the approval in writing of the Australian Statistician).

of a particular person or organisation, while s 13(3) provides that information about a person shall not be disclosed under s 13(1) in a manner that is likely to enable the identification of that person.

Electoral information

2.81 The *Commonwealth Electoral Act 1918* (Cth) requires the Australian Electoral Commission (AEC) to construct and maintain a roll of people eligible to vote at federal—and, by agreement, most state and local government—elections. Electoral rolls are available for public inspection without fee at offices of the AEC.[116] Only the names and addresses of enrolled voters are included on the publicly available electoral roll.

2.82 A publicly available electoral roll facilitates the conduct of free and fair elections by 'enabling participants to verify the openness and accountability of the electoral process and object to the enrolment of any elector'.[117] In addition, the *Commonwealth Electoral Act* allows for the disclosure of electoral information to a number of people and bodies. For example, Members of Parliament, political parties and approved medical researchers may be provided with electoral information.[118] This information may only be used for certain purposes.[119]

2.83 However, the *Commonwealth Electoral Act* also contains secrecy provisions aimed at protecting the unauthorised disclosure of electoral information. Section 90B prohibits the disclosure of certain information, such as information about defence and AFP personnel, to anyone.[120] Section 91B of the Act makes it an offence for a person to disclose information obtained under s 90B unless the disclosure 'would be a use of the information for a permitted purpose under s 91A'. Section 189B makes it an offence to disclose information obtained from an electronic list of postal vote applicants provided by the AEC if the disclosure 'would not be a use of the information for a permitted purpose'. Finally, s 323 makes it an offence for an officer or scrutineer to disclose any information with respect to the vote of an elector that was acquired under the Act or regulations in a manner that is likely to enable the identification of the elector.

Defence or security information

2.84 A number of Commonwealth secrecy provisions aim to prevent the unauthorised disclosure of defence or security information. It is often argued that secrecy is of vital importance in protecting this type of information. However, 'perennial leaks have ensured that secrecy in defence matters is an almost routine source of governmental

---

116 *Commonwealth Electoral Act 1918* (Cth) s 90A.

117 Australian Electoral Commission, *How to View the Commonwealth Electoral Roll* <http://www.aec.gov.au/Enrolling_to_vote/About_Electoral_Roll/> at 6 November 2008.

118 *Commonwealth Electoral Act 1918* (Cth) s 90B.

119 Ibid s 91A.

120 Ibid s 90B (6), (7), (8A).

concern'.[121] Most of the secrecy provisions that protect defence or security information criminalise the unauthorised disclosure of this information.

2.85 Some of the provisions that protect defence or security information do so by expressly prohibiting the disclosure of certain information. For example, s 73A of the *Defence Act 1903* (Cth) makes it an offence for a member of the Australian Defence Force, or a person engaged or appointed under the *Public Service Act*, to communicate, otherwise in the course of his or her official duty,

> any plan, document, or information relating to any fort, battery, field work, fortification, or defence work, or to any defences of the Commonwealth, or to any factory, or air force aerodrome or establishment or any other naval, military or air force information.

2.86 Other provisions prohibit the disclosure of any information if the disclosure 'is likely to' prejudice the security or defence of Australia.[122] In some provisions, the threshold question of whether information will prejudice the security or defence of Australia is determined by a designated person. 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'.[123]

2.87 Section 91.1 of the *Criminal Code* (Cth), dealing with espionage, also falls into this category. This provision makes it an offence for a person to disclose information concerning the security or defence of the Commonwealth with the intention of prejudicing the security or defence of the Commonwealth, or of giving an advantage to another country's security or defence. Section 90.1 provides that the term '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'.

Law enforcement and intelligence information

2.88 A number of secrecy provisions aim to protect information about the operations or investigations of law enforcement agencies. It has been argued that secrecy is an 'indispensible operational technique' for law enforcement agencies.[124] As Campbell notes, it would be

> quite ridiculous to expect police forces to detect and apprehend criminals if everyone, including the suspects, were permitted to examine the documents describing the

---

121 G Terrill, *Secrecy and Openness: The Federal Government from Menzies to Whitlam and Beyond* (2000), 228.

122 See, eg, *Defence Force Discipline Act 1982* (Cth) s 58.

123 See also *Auditor-General Act 1997* (Cth) s 37; *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24; *Patents Act 1990* (Cth) s 173; *Privacy Act 1988* (Cth) s 70.

124 E Campbell, 'Public Access to Government Documents' (1976) 41 *Australian Law Journal* 73, 76.

> strategies to be followed in combating crime and police reports on investigations in progress. Informers whose names and statements appeared on the records would be deterred from coming forward for fear of retaliation.[125]

2.89 Further, in relation to intelligence information, it has been noted that:

> any betrayal by an intelligence officer of his or her duty to keep confidential information secure, irrespective of the objective value of the information in question, can lead to loss of confidence by cooperating agencies in the ability of the Australian intelligence agencies to maintain security.[126]

2.90 Secrecy provisions prohibit the unauthorised disclosure of a wide range of law enforcement and intelligence information. Some simply prohibit the disclosure of information if its disclosure could prejudice the conduct of an investigation or inquiry.[127] Others identify specific types of protected information, such as information about: the existence of a law enforcement operation or investigation;[128] the existence or content of a warrant;[129] the questioning or detention of a person in connection with a warrant;[130] the identity of an intelligence officer;[131] and the identity of a participant in the National Witness Protection Program.[132]

2.91 Further, financial intelligence information collected under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) is protected from unauthorised disclosure,[133] as is information intercepted or accessed under the *Telecommunications (Interception and Access) Act 1979* (Cth)[134] or obtained under the *Surveillance Devices Act 2004* (Cth).[135] Some secrecy provisions also prohibit the unauthorised disclosure of information obtained when conducting a forensic procedure on a suspect, offender or volunteer.[136]

Confidential information

2.92 A number of the secrecy provisions identified by the ALRC aim to prevent the unauthorised disclosure of confidential information. Some do this by simply prohibiting the disclosure of 'confidential' information, which may or may not be

---

125 Ibid, 76.
126 *R v Lappas* (2003) 152 ACTR 7, [22].
127 See, eg, *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1); *Australian Crime Commission Act 2002* (Cth) s 9; *Privacy Act 1988* (Cth) s 70.
128 *Australian Crime Commission Act 2002* (Cth) ss 29B (1), (3).
129 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS; *Telecommunications (Interception and Access) Act 1979* (Cth) ss 63, 133.
130 *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS.
131 Ibid s 92; *Intelligence Services Act 2001* (Cth) s 41.
132 *Witness Protection Act 1994* (Cth) s 22.
133 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 121, 122, 123, 127, 128, 130, 131.
134 *Telecommunications (Interception and Access) Act 1979* (Cth) s 63, 133.
135 *Surveillance Devices Act 2004* (Cth) s 45.
136 See, eg, *Crimes Act 1914* (Cth) s 23YO.

defined in the Act.[137] Others do this by prohibiting the disclosure of information that was supplied in confidence,[138] or information the disclosure of which would constitute a breach of confidence.[139]

2.93 Other secrecy provisions identified by the ALRC aim to protect a specific type of confidential information—that is, confidential commercial information.[140] The public policy which underlies these provisions is

> the need to ensure that people do not take improper advantage or suffer unjust consequences by reason of their disclosure to the Commonwealth and its agencies of matters that would normally be regarded as business confidences, simply because they wish to secure the benefits and incentives [provided for by an Act].[141]

2.94 Some of these provisions specify the type of confidential commercial information protected. For example, s 162 of the *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) prohibits the disclosure of confidential commercial information about an active constituent for a proposed or existing chemical product, a chemical product or any of its constituents, or a label for containers for a chemical product. Others prohibit the disclosure of information obtained under an Act on the basis that its disclosure would be detrimental to the commercial interests of a person or body. For example, s 74 of the *Wheat Export Marketing Act 2008* (Cth) prohibits the disclosure of 'protected confidential information', which is defined as information provided under certain provisions of the Act, the disclosure of which could cause financial loss or detriment to a person or benefit a competitor of the person.[142]

Indigenous sacred or sensitive information

2.95 A small number of Commonwealth secrecy provisions prohibit the disclosure of information that is considered sacred or otherwise significant by Indigenous peoples. For example, s 193S(3)(b) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth) prohibits the disclosure by a designated person[143] of any information if he or she is: (a) aware that it is considered sacred or otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders; and (b) 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 or the Council of the Institute must not disclose

---

137 *Water Act 2007* (Cth) s 215; *Offshore Minerals Act 1994* (Cth) s 374.

138 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32; *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) ss 604–15, 604–20; *Therapeutic Goods Act 1989* (Cth) s 9C.

139 *Industry Research and Development Act 1986* (Cth) s 47(1). Breach of confidence is discussed further in Ch 1.

140 See, eg, *Agricultural and Veterinary Chemicals Code Act 1994* (Cth) s 162(1); *Gene Technology Act 2000* (Cth) s 187.

141 *Foley v Tectran Corporation Pty Ltd* (1984) 57 ALR 26, 31.

142 *Wheat Export Marketing Act 2008* (Cth) s 73. See also *Auditor-General Act 1997* (Cth) s 37.

143 As defined in s 193S(1) of the Act.

information if the disclosure would be inconsistent with the views or sensitivities of relevant Aboriginal persons or Torres Strait Islanders.[144]

Other information

2.96 The ALRC has also identified secrecy provisions that aim to protect other types of Commonwealth information, including information that:

- would disclose the deliberations of the Cabinet;[145]
- would disclose the deliberations or advice of the Executive Council;[146]
- would prejudice the international relations of the Commonwealth;[147]
- would prejudice relations between the Commonwealth and a state;[148]
- could form the basis for a claim by the Crown in right of the Commonwealth in a judicial proceeding that the information should not be disclosed;[149]
- is derived from, or related to, a complaint;[150]
- would endanger the safety of any person;[151]
- relates to an alternative dispute resolution process;[152]
- is derived from inspecting records;[153]
- would reveal that a person was acting in a certain capacity;[154] and
- relates to an investigation conducted by a safety compliance agency.[155]

---

144 See also *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3)(d).

145 *Auditor-General Act 1997* (Cth) s 37(1), (2)(b); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(c); *Privacy Act 1988* (Cth) s 70.

146 *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(d); *Privacy Act 1988* (Cth) s 70.

147 *Auditor-General Act 1997* (Cth) s 37(1), (2)(a); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(a); *Privacy Act 1988* (Cth) s 70.

148 *Auditor-General Act 1997* (Cth) s 37(1), (2)(c); *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(b); *Privacy Act 1988* (Cth) s 70.

149 *Auditor-General Act 1997* (Cth) s 37(1), (2)(f).

150 *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63; *Sex Discrimination Act 1984* (Cth) s 92(1).

151 *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 24(1)(h); *Australian Crime Commission Act 2002* (Cth) s 9; *Privacy Act 1988* (Cth) s 70.

152 *Workplace Relations Act 1996* (Cth) ss 702, 707, 712, 715, sch 6, cl 38(5).

153 Ibid sch 1, cl 276; *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) s 183–1(b); *Copyright Act 1968* (Cth) (Cth) s 203E(10).

154 *Workplace Relations Act 1996* (Cth) ss 165, 425, 485, 486, 668(3)(f).

155 *Transport Safety Investigation Act 2003* (Cth) ss 53, 60; *Civil Aviation Act 1988* (Cth) s 32AP; *Space Activities Act 1998* (Cth) s 96.

Question 2–4 Given that the consolidation of secrecy laws is being considered in relation to taxation secrecy and disclosure provisions, in what other legislative areas, if any, is this appropriate?

Question 2–5 Should Commonwealth secrecy provisions aim to protect:

(a) specific types of information? If so, what types of information should be protected by the provisions?

(b) information held by certain persons or agencies? If so, which persons or agencies should be regulated by the provisions?

(c) information, the disclosure of which may harm a specified public interest? If so, what public interest or interests should be protected by the provisions?

Form of secrecy provisions

2.97 As noted above and in Chapter 1, Commonwealth secrecy provisions take many forms and exhibit a 'bewildering diversity of drafting styles'.[156] In this section, the ALRC considers the general form of the provisions. Particular aspects of form—such as those related to penalties, exceptions and defences—are discussed in later chapters.

2.98 Many secrecy provisions contain a general prohibition on disclosure of certain information and then attempt to set out a detailed 'code' that defines the circumstances in which disclosure is allowed.[157] For example, s 34 of the *Dental Benefits Act 2008* (Cth) makes it an offence for a person regulated by the provision to disclose protected information. Sections 35–41 then set out the circumstances in which disclosure of protected information is authorised. In relation to provisions such as these, McGinness notes that:

> any attempt to include such a code leads to further complexity in a secrecy provision and results in regular demands for amendment to deal with changing criteria for information sharing within government.[158]

2.99 In *Jackson v Magrath*, Dixon J noted that the lengthy provisions in s 16 of the *Income Tax Assessment Act 1936* (Cth) showed 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

156 I Eagles, 'Public Interest Immunity and Statutory Privilege' (1983) 42 *Cambridge Law Journal* 118, 118.
157 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.
158 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 62.

> fiscal and other government departments has proved a recurring problem for the draftsman. It is apparent that no ready formula has been found for its solution. [159]

2.100 As noted above, the Taxation Secrecy Review proposed that the various taxation secrecy and disclosure provisions be standardised so that they clearly describe the information to be protected and by whom; and identify to whom protected information can be disclosed, the circumstances in which disclosure is allowed and the purposes for which disclosed information can be used.[160]

2.101 The ALRC is interested in stakeholder views on whether this form of secrecy provision is appropriate.

Question 2–6 Should secrecy provisions establish a general prohibition on disclosure of certain information and then attempt to codify the circumstances in which disclosure is allowed?

2.102 While many Acts contain a single consolidated provision, division or part dealing with secrecy or confidentiality, a different approach has been adopted in some cases. The *Veterans Entitlements Act 1986* (Cth), for example, contains a number of secrecy provisions in similar terms in relation to each of the different pension entitlements. Section 35H(7)(a) deals with disclosure of confidential information in determinations in relation to service pensions; s 36L(8)(a) deals with disclosure of confidential information in determinations in relation to age service pensions; s 37L(8)(a) deals with disclosure of confidential information in determinations in relation to invalidity service pensions; s 38L(8)(a) deals with disclosure of confidential information in determinations in relation to partner service pensions; and s 45Q(8)(a) deals with disclosure of confidential information in determinations in relation to income support supplements. All of the provisions are in very similar terms.

2.103 This approach appears to give rise to unnecessary duplication. The ALRC is interested in stakeholder views on whether this approach is desirable or necessary in some situations, or whether it would be better to consolidate such secrecy provisions into a single provision, where possible.

---

159 *Jackson v Magrath* (1947) 75 CLR 293, 312.

160 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), [2.3].

Question 2–7 Should secrecy provisions be consolidated, wherever possible, into a single provision in each Act or regulation?

Question 2–8 Are there any other issues in relation to the form of secrecy provisions that the ALRC should consider in the course of this Inquiry?

3. Secrecy Provision Elements

Contents

Introduction

3.1 The nature of secrecy provisions has come under scrutiny on a number of occasions over the past 30 years. In particular, in *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98), the Australian Law Reform Commission (ALRC) made the following recommendations:

> The Australian Government should review all legislative and regulatory provisions giving rise to a duty not to disclose official information—including in particular regulation 2.1 of the *Public Service Regulations*—to ensure that the duty of secrecy is imposed only in relation to information that genuinely requires protection and where unauthorised disclosure is likely to harm the public interest.[1]

3.2 Chapter 2 provides an overview of secrecy provisions in Commonwealth legislation, including the different types of information that these provisions are designed to protect and the array of drafting styles they exhibit. This chapter focuses upon principal elements of the secrecy provisions—*whose activity* is regulated by Commonwealth secrecy provisions, and *what kind of activity* is regulated. In addition, the chapter examines the extent to which such provisions should be limited to conduct that is likely to harm the public interest and whether existing provisions are consistent with the *Australian Constitution.*

---

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

Whose activity is regulated?

3.3 A key issue in the operation of secrecy provisions is who is caught by them—including what kind of employment relationship exists and when bodies corporate are included. A particularly difficult issue concerns the 'post-employment province'[2] of secrecy provisions.

The range of parties regulated

3.4 As discussed in Chapter 2, reg 2.1 of the *Public Service Regulations* sets out the general duty of an 'APS employee' not to disclose official information. An APS employee is defined in s 7 of the *Public Service Act* to mean a person engaged under s 22—that is, a person engaged by an Agency Head for the purposes of the agency—or 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.

3.5 Section 70 of the *Crimes Act* regulates conduct by 'Commonwealth officers'.[3] The term 'Commonwealth officer' includes, but is wider than, 'APS employees' and is defined in the *Crimes Act* to mean:

> a person holding office under, or employed by, the Commonwealth and includes:
>
> (a) a person appointed or engaged under the *Public Service Act 1999*;
>
> (aa) a person permanently or temporarily employed in the Public Service of a Territory or in, or in connection with, the Defence Force, or in the Service of a public authority under the Commonwealth;
>
> (b) the Commissioner of the Australian Federal Police, a Deputy Commissioner of the Australian Federal Police, an AFP 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.[4]

---

2 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 251.
3 The definition of a 'Commonwealth officer' is also discussed in Ch 2.
4 *Crimes Act 1914* (Cth) s 3.

3.6 While reg 2.1 and s 70 regulate the conduct of 'APS employees' and 'Commonwealth officers' respectively, other secrecy provisions expressly refer to a wider range of individuals, reflecting changes to the structure of government and government service provision. Other parties expressly regulated include consultants[5] and others who provide goods and services to the Australian Government.[6] Some provisions also extend to state and territory government employees and local government employees.[7]

3.7 In 1990, John McGinness noted the growth in statutory authorities with power to require the production of information and the related growth in secrecy provisions applying to those authorities.[8] Such provisions often bind the head and staff of the statutory authority, but also may bind those who enter into arrangements with such an authority.[9]

3.8 A number of provisions also direct the behaviour of individuals working in federally regulated areas of the private sector—for example, aged care providers[10] and financial institutions.[11]

3.9 It is important to note that bodies corporate, as well as individuals, may be found guilty of a criminal offence. Part 2.5 of the *Criminal Code* (Cth) deals with corporate criminal responsibility. Section 12.2 provides that where a physical element of an offence is committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of his or her employment, or within his or her actual or apparent authority, that physical element must also be attributed to the body corporate. Section 12.3 provides that where it is necessary to prove intention, knowledge or recklessness in relation to the physical element of the offence, the fault element must be attributed to the body corporate that expressly, tacitly or impliedly authorised or permitted the commission of the offence.

3.10 In its submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into the protection of confidential personal and commercial information held by the Commonwealth, the Attorney-General's Department noted that confidentiality clauses were included in contracts with service providers as a matter of course.[12] Having acknowledged this practice, the Committee

---

5 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32.
6 See, eg, *Customs Administration Act 1985* (Cth) s 16.
7 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.
8 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 49.
9 See, eg, *Australian Institute of Health and Welfare Act 1987* (Cth) s 29.
10 See, eg, *Aged Care Act 1997* (Cth) s 62–1.
11 See, eg, *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 123.
12 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 53.

nonetheless recommended that the *Privacy Act 1998* (Cth) should be amended to ensure that contractors to Commonwealth agencies were bound by the same privacy principles as the agency itself.[13] The Committee was of the view that information should be protected at every point on the distribution chain including where that information is handled outside the public sector.[14]

3.11 The ALRC is interested in stakeholder views on the circumstances in which secrecy provisions should regulate the behaviour of persons other than Commonwealth officers such as: consultants and others who provide goods and services to the Australian Government; those who enter into arrangements with the Australian Government; and state and territory government employees.

Question 3–1 In what circumstances should secrecy provisions regulate the behaviour of persons other than Commonwealth officers such as: consultants and others who provide goods and services to the Australian Government; those who enter into arrangements with the Australian Government; and state and territory government employees?

3.12 A number of secrecy provisions, in particular those relating to defence and national security, regulate the activities of *any* person who comes into possession or control of documents or information.[15] Section 79 of the *Crimes Act*, for example, prohibits unauthorised handling or communication of official secrets by any person, including members of the media.

3.13 Unsurprisingly, this has been the subject of comment. As noted by the then Attorney-General, the Hon Daryl Williams AM QC, MP in introducing the Criminal Code Amendment (Espionage and Related Offences) Bill 2002:

> There has been considerable media attention focused on the perceived impact that the official secrets provisions … were alleged to have on freedom of speech and on the reporting of government activities.[16]

3.14 Very wide provisions may need reconsideration following the decision in *Bennett v President, Human Rights and Equal Opportunity Commission*.[17] In *Bennett*, Finn J struck down a 'catch all' secrecy provision that did not appropriately balance the need to protect Commonwealth information with the implied constitutional freedom to communicate on government and political matters.[18] The ALRC is interested in

13 Ibid, Rec 16.
14 Ibid, [7.11.2].
15 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9(2).
16 Commonwealth, *Parliamentary Debates*, House of Representatives, 13 March 2002, 1111 (D Williams—Attorney-General).
17 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119.
18 Ibid. The decision in *Bennett* is also discussed in Ch 1 and below.

stakeholder views on whether statutory secrecy provisions should extend to regulate the behaviour of 'any person' including members of the media.

Question 3–2 Some secrecy provisions—for example a number of provisions relating to defence and security—regulate the activities of anyone who comes into possession or control of documents or information. When should secrecy provisions regulate the behaviour of 'any person', including members of the media?

Current and former parties

3.15 A number of secrecy provisions expressly regulate the behaviour of persons who have access to Commonwealth information because of their current position, as well as those who have had access in the past but may no longer have access. For example, s 70 of the *Crimes Act* regulates the behaviour of persons who are current *and former* Commonwealth officers.

3.16 An example of a more specific secrecy provision governing both current and former officers is s 191 of the *Aboriginal and Torres Strait Islander Act 2005* (Cth), which expressly applies to a person:

> (a) who is or has been an Indigenous Business Australia Director or acting Indigenous Business Australia Director;
>
> (b) who is or has been the Indigenous Business Australia General Manager or an acting Indigenous Business Australia General Manager;
>
> (c) who is or has been employed or engaged under section 175 or 178;
>
> (d) who is performing, or who has performed, duties on behalf of Indigenous Business Australia pursuant to an arrangement under section 176; or
>
> (e) whose services are being or have been made available to Indigenous Business Australia pursuant to an arrangement under section 177.

3.17 The *Archives Act 1983* (Cth) may also apply to former officers. Section 30A(1) 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).

3.18 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 1999* (Cth)[19] and therefore fall within the definition of 'Commonwealth officers' 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 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'—in this case, census information that is not in the open access period—without lawful authority or excuse.

3.19 The common law duty of fidelity and loyalty[20] that an employee owes to an employer also offers a degree of protection to information acquired during the employment relationship, even after that relationship has come to an end. 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:

> The complexity inherent in striking a balance between these conflicting principles is particularly acute where an employee in the course of managerial or administrative duties acquires information concerning the employer's business or practices which makes that employee attractive to other potential employers. Persons in public sector employment who have knowledge of the business practices of governments are often keenly sought by the private sector for this reason. Indeed, it is not infrequent that public sector employees are recruited by non-government bodies on the basis that they possess knowledge and expertise which could only, or largely, be acquired as a consequence of the person's employment in government.[21]

3.20 Tsaknis argues 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'.[22] Paul Finn agrees, stating that this provision is 'objectionably wide in its scope and mysterious in its possible applications'.[23]

3.21 A secrecy obligation that is limited to the period of employment or engagement will obviously not provide adequate protection. Finn notes, however, that:

> What properly can be expected of an ex-officer, likewise, is necessarily affected by the consideration that, no longer a 'public servant', the ex-officer now has legitimate private and personal interests of which account needs be taken in giving secrecy its post-employment province. In other words, the secrecy demands that can properly be made of an officer are not on all fours with those that can be made of an ex-officer.[24]

---

19 *Archives Act 1983* (Cth) s 9.
20 The common law duty is discussed further in Ch 1.
21 L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18 *Criminal Law Journal* 254, 262.
22 Ibid, 262.
23 P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991), 259.
24 Ibid, 251.

3.22 Finn describes the common law duty developed in the context of private sector employment:

> If the information in question can fairly be regarded as a separate part of the employee's stock of knowledge which a person of ordinary honesty and intelligence would recognise to be the property of the old employer, it will be protected. If, however, it merely constitutes knowledge, skill and experience which, as a result of the previous employment, has become the employee's own, it will not.[25]

3.23 Finn's view is that this duty may not be directly applicable in the public sector. He discusses applying the duty in the public sector context to different categories of government information, for example, third party information, commercial information, and other government information. He expresses the view that third party and commercial information should be protected—while it remains confidential and not in the public domain—but suggests that, in relation to other government information it should only be protected to the extent that disclosure is likely to injure the public interest.[26]

3.24 The ALRC is interested in stakeholder views on the circumstances in which it is appropriate for secrecy provisions to continue to regulate the behaviour of those who have been Commonwealth officers, or who have held other positions subject to Commonwealth secrecy provisions, but who are no longer in those positions.

Question 3–3 In what circumstances should secrecy provisions regulate those who have been Commonwealth officers, or who have held other positions subject to Commonwealth secrecy provisions, but who are no longer in those positions?

What kind of activity is regulated?

The range of activity regulated

3.25 Secrecy provisions in federal legislation not only regulate the disclosure of Commonwealth information but also a range of other activities. Certain provisions prohibit unauthorised soliciting[27] or receipt[28] of information, as well as obtaining,[29]

25 Ibid, 253.
26 Ibid, 257.
27 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 165.
28 See, eg, *Crimes Act 1914* (Cth) s 79(6).
29 See, eg, *A New Tax System (Family Assistance)(Administration) Act 1999* (Cth) s 163.

possessing,[30] making a record of,[31] or using[32] information. Disclosing information is also described as divulging[33] or communicating[34] information.

3.26 The House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into the protection of confidential personal and commercial information recommended that unauthorised dealing in confidential information held by the Commonwealth should be prohibited at every point on the 'distribution chain'[35]—or information flow, as the ALRC describes it in Chapter 1. The Committee noted that the confidentiality provisions in the *Social Security Act 1991* (Cth) prohibit unauthorised access to protected information; unauthorised use of protected information—including disclosing, recording or otherwise using—soliciting the disclosure of protected information; offering to supply protected information; and holding oneself out as being able to supply protected information.[36]

3.27 Some provisions focus on obtaining information. For example, under s 1312 of the *Social Security Act*, a person also 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.

3.28 Further, under s 91(3) of the *Criminal Code*, a person commits an offence where the person makes, *obtains* or copies a record (in any form) of information concerning the Commonwealth's security or defence (or that of another country obtained from the Commonwealth); and does so intending that the record will, *or may*, be delivered to another country intending to prejudice the Commonwealth's security or defence.

3.29 Other provisions are concerned with the receipt of information. Section 79(5) of the *Crimes Act* states:

> 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.[37]

---

30 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9.
31 See, eg, *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30.
32 See, eg, *Aged Care Act 1997* (Cth) s 62–1.
33 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32.
34 See, eg, *Defence (Special Undertakings) Act 1952* (Cth) s 9.
35 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), Rec 31.
36 Ibid, [7.11.3].
37 Section 79(6) creates a similar offence in relation to material that is in contravention of s 79(3).

3.30 The House of Representatives Standing Committee cautioned against the creation of offences prosecuting the mere possession or receipt of confidential information. In its 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'.[38]

3.31 McGinness argues that provisions that criminalise the mere receipt of information may unduly burden journalists who may receive information they have no intention of publishing or members of parliament who may be briefed by public servants without authorisation. He notes that s 5 of the *Official Secrets Act 1989* (UK) does not contain offences of mere unlawful possession or receipt of official information.[39]

Question 3–4 Should secrecy provisions regulate only the disclosure of information or is it appropriate to regulate other conduct such as the unauthorised receipt, collection, use or recording of information?

Initial and subsequent disclosures

Information disclosed with authority

3.32 A number of secrecy provisions regulate both the initial and any subsequent unauthorised handling of Commonwealth information. For example, under s 23E of the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth):

> (4) A person commits an offence if:
>
> (a) information is communicated to the person (the *first person*) in accordance with [the Act]; and
>
> (b) the information is communicated by a person (the *second person*) to whom this section applies; and
>
> (c) the second person acquired the information because of his or her membership of, or employment by, a Land Council or his or her activities as an authorised person; and
>
> (d) the information concerns the affairs of a third person; and
>
> (e) the first person, either directly or indirectly, makes a record of, or divulges or communicates the information to any other person.

38 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), [7.11.7].

39 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 85.

3.33 Under s 86–3 of the *Aged Care Act 1997* (Cth), the Secretary of the Department of Health and Ageing may disclose protected information in certain circumstances, including to other government departments—such as Centrelink and Medicare—or where there is a risk to health and safety. Under s 86–5, it is an offence for a person who receives information by virtue of s 86–3 to make a record of, disclose or otherwise use the information other than for the purpose for which the information was disclosed.

3.34 McGinness notes that:

> Where a secrecy provision permits disclosure to other government agencies then, in the absence of a specific provision, the persons receiving the information are not bound by that statute to maintain its confidentiality … Some secrecy provisions attempt to deal with this by imposing a further prohibition on disclosure by recipients.[40]

3.35 However, the vast majority of secrecy provisions mapped by the ALRC to date do not contain a prohibition on disclosure by recipients. A 2006 Treasury review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review) proposed that a person who is given information under secrecy and disclosure provisions should also be subject to strict secrecy requirements. It stated that such a requirement would be consistent with the principles of disclosure to third parties found under the *Privacy Act*.[41]

3.36 It is important to note, however, that not all information which is considered secret at some point requires protection from third party disclosure. For example, information that was obtained by an agency, such as the Australian Bureau of Statistics, that is transformed into non-identifiable statistical information would not need further protection.[42]

Information disclosed without authority

3.37 A different set of issues may arise when protected information is disclosed to a person who does not have authority to receive it. The common law provides some protection for confidential information disclosed to a third party who knows, or has reason to know, that protected information has been supplied to him or her in breach of confidence.

3.38 McGinness notes, however, the limitations of the common law in dealing with unauthorised disclosure of official information: while the receipt of official information

---

40 Ibid, 64.

41 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 14. Information Privacy Principle 11.3 states that the recipient of information can only use or disclose that information for the purpose for which it was disclosed to that recipient: *Privacy Act 1988* (Cth) s 14.

42 For example, the *Privacy Act* only applies to information 'about an individual whose identity is apparent or can be reasonably ascertained': *Privacy Act 1988* (Cth) s 6(1). See also Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [6.2]–[6.6].

may be an offence, the Commonwealth has no right to obtain an injunction to restrain publication.[43] This issue is discussed further in Chapter 6.

3.39 As noted above, the House of Representatives Standing Committee expressed the view that the general offence provisions should prohibit unauthorised dealing in confidential third party information at every point in the 'distribution chain' where that person has the requisite mental element.[44]

3.40 The Review of the Commonwealth Criminal Law, chaired by Sir Harry Gibbs (the Gibbs Committee) recommended that Australian legislation should follow the *Official Secrets Act* (UK) in including a provision preventing a person from disclosing information they know to have been unlawfully obtained. The Gibbs Committee recommended the following form of words for the offence:

> Where a person knows, or has reasonable grounds to believe, that information—
>
> i. had been disclosed (whether to him or another) by a Commonwealth officer or government contractor without authority or had been unlawfully obtained from either such person; or
>
> ii. had been entrusted to him or her in confidence by such officer or contractor on terms requiring it to be held in confidence; or
>
> iii. had been disclosed (whether to him or another) without lawful authority by a person to whom it had been entrusted as in (ii);
>
> it would be an offence for the person to disclose the information without authority, knowing or having reasonable cause to believe that the disclosure would be damaging.[45]

3.41 The ALRC is interested in stakeholder views on whether secrecy provisions should, as a matter of course, include offences dealing with both the initial unauthorised handling of information and any subsequent disclosures.

Question 3–5 Should all secrecy provisions seek to regulate both initial and subsequent unauthorised handling of Commonwealth information?

---

43 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 85.

44 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), [7.11.7].

45 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 333.

The elements of criminal offences

3.42 The vast majority of the secrecy provisions identified by the ALRC to date establish criminal offences. The ALRC has identified only one civil penalty provision so far.[46]

3.43 A small number of provisions identified by the ALRC do not criminalise the wrongful handling of Commonwealth information but rather establish rules for the handling of this information, the breach of which can lead to the imposition of an administrative penalty.[47] A breach of these types of rules does not generally involve a requirement to prove fault. As such, this section will focus on the elements required for criminal offences, and, in particular, the fault elements.

3.44 Criminal offences, whether in statute or common law, are considered to be made up of physical and mental elements, also described as the prohibited act (*actus reus*) and the criminal mental element (*mens rea*). In the *Criminal Code*, these elements are called 'physical elements' and 'fault elements'.

3.45 Criminal offences may be structured in one of three ways:

- offences that have both physical elements and fault elements;
- strict liability offences: where the prosecution is not required to prove any fault elements but where a defence of honest and reasonable mistake of fact, and possibly other statutory defences (such as due diligence), are available; and
- absolute liability offences: where the prosecution is not required to prove any fault elements, and the defence of honest and reasonable mistake of fact is not available.

3.46 The *Criminal Code* contains general principles of criminal responsibility under the laws of the Commonwealth.[48] The Code is aimed at ensuring that the same principles of criminal responsibility apply to all Commonwealth offences. Commonwealth legislation creating an offence must be read alongside the *Criminal Code* to fully understand a person's legal rights and obligations.

Physical elements

3.47 The *Criminal Code* stipulates that the physical elements of an offence may be conduct; a result of conduct; or a circumstance in which conduct, or a result of conduct, occurs.[49] 'Conduct' means an act, an omission or state of affairs.[50]

---

46 *Workplace Relations Act 1996* (Cth) sch 1, s 276. Civil penalty provisions are discussed in Ch 5.
47 See Ch 2.
48 *Criminal Code* (Cth), Ch 2.
49 Ibid s 4.1(1).
50 Ibid s 4.1(2).

Fault elements

3.48 The *Criminal Code* provides that fault elements may include intention, knowledge, recklessness or negligence, but that particular offences may specify other fault elements.[51]

3.49 Under the *Criminal Code*, if the legislation creating an offence does not specify a fault element for a physical element consisting of conduct, the fault element is intention.[52] Where an offence provision does not specify a fault element for a physical element consisting of a circumstance or a result, the fault element is recklessness.[53]

3.50 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* refers to the background to these provisions:

> In the process of harmonising Commonwealth criminal law with the Criminal Code, a much wider range of fault and no fault terminology were removed from the statute book. Use of the Criminal Code elements is designed to remove ambiguities that had been present in much of the alternative terminology used, and provides a much simpler basis for understanding and applying Commonwealth offences, including by providing a clearer and firmer basis for any prosecution.
>
> Identification of the elements of Commonwealth criminal offences in legislation should consistently use the terms, and rely on the meanings of those terms, provided in the Criminal Code.[54]

Intention and recklessness

3.51 Intent is the most common fault element. A person's intention may be to undertake an act (such as the intention to enter premises) or to bring about a consequence (intention to cause death). Section 5.2 of the *Criminal Code* provides that:

> (1) A person has intention with respect to conduct if he or she means to engage in that conduct.
>
> (2) A person has intention with respect to a circumstance if he or she believes that it exists or will exist.
>
> (3) A person has intention with respect to a result if he or she means to bring it about or is aware that it will occur in the ordinary course of events.

3.52 A person is 'reckless' where he or she is indifferent whether a substantial or foreseeable risk will eventuate. Section 5.4 of the *Criminal Code* provides that:

---

51 Ibid s 5.1. For example, the *Criminal Code* itself stipulates an additional fault element of 'dishonesty' in relation to offences in Ch 7—*The Proper Administration of Government*. Dishonesty is defined as 'dishonest according to the standards of ordinary people' and 'known by the defendant to be dishonest according to the standards of ordinary people': s 130.3.

52 Ibid s 5.6(1).

53 Ibid s 5.6(2).

54 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 20–21.

> (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.

3.53 The ALRC's mapping exercise to date indicates that the majority of Commonwealth secrecy provisions do not stipulate fault elements. In these circumstances, intention as to conduct and recklessness as to circumstances or results will be the default position by virtue of the *Criminal Code*.

3.54 An example of such a provision is s 30(2) of the *A New Tax System (Australian Business Number) Act 1999* (Cth), which simply provides that the 'entrusted' person:

> (a) must not make a record of protected information; and
>
> (b) must not disclose it to anyone else;
>
> if the recording or disclosure is not done in accordance with subsection (3).

3.55 Section 30(3) then sets out a range of circumstances in which it is not an offence to make a record or disclose such information, for example, where the recording or disclosure is for the purposes of the Act;[55] or where the recording or disclosure happens in the course of the performance of the duties of the entrusted person's official employment.[56] In this example, making a record or disclosing protected information is the conduct. As the provision does not specify a fault element for this conduct, the fault element is intention implied under the *Criminal Code*.

3.56 In contrast, recklessness is the fault element expressly provided for under s 23YO of the *Crimes Act*:

> (1) A person is guilty of an offence if:
>
> (a) the person has access to any information stored on the Commonwealth DNA database system or NCIDD [National Criminal Investigation DNA Database] or to any other information revealed by a forensic procedure carried out on a suspect, offender or volunteer; and

55 *A New Tax System (Australian Business Number) Act 1999* (Cth) s 30(3)(a).
56 Ibid s 30(3)(b).

> (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.

3.57 Under the criminal law, those who intend to bring about a particular consequence 'are generally regarded as having the most blameworthy state of mind'.[57] However, this is not always the case, and in some secrecy provisions there is not a larger penalty for those who intend to bring about a consequence compared to those who act recklessly. For example, s 23YO set out above, attracts a maximum penalty of two years imprisonment. Section 63 of the *Telecommunications (Interception and Access) Act 1979* (Cth)—which prohibits unauthorised disclosure of information obtained by intercepting a communication—has intent as the mental element and also attracts a maximum penalty of two years imprisonment.[58]

Knowledge

3.58 Under s 5.3 of the *Criminal Code*, a person has knowledge of a circumstance or a result if he or she is aware that it exists or will exist in the ordinary course of events. An example of an offence where knowledge forms part of the mental element is s 130 of the *Health Insurance Act 1973* (Cth). Under that section where a person solicits the unauthorised disclosure of protected information from an officer or another person; and knows or ought reasonably to know that the information is protected information, he or she is guilty of an offence—whether or not any protected information is actually disclosed.

Negligence

3.59 Criminal negligence concerns what a reasonable person would have been aware of at the time of the relevant act or omission, rather than what the accused was actually aware of. Section 5.5 of the *Criminal Code* provides that:

> A person is negligent with respect to a physical element of an offence if his or her conduct involves:
>
> (a) such a great falling short of the standard of care that a reasonable person would exercise in the circumstances; and
>
> (b) such a high risk that the physical element exists or will exist;
>
> that the conduct merits criminal punishment for the offence.

3.60 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that negligence should only be used as a fault element where it is justified in the particular circumstances, such as where:

---

57 D Brown, D Farrier, S Egger and L McNamara, *Criminal Laws* (3rd ed, 2001), 377.

58 Note s 63 is read in conjunction with s 105 of the *Telecommunications (Interception and Access) Act 1979* (Cth). Penalties are discussed further in Chapter 5.

- the context is one where negligence is a well established indication of liability (for example, in an area such occupational health and safety); or

- a person was not aware of relevant risks or circumstances but is deserving of criminal punishment because he or she falls seriously short of the requisite standard of care.[59]

3.61 To date, the ALRC has not identified any secrecy provisions imposing a fault element of negligence. However, s 79(4)(c) of the *Crimes Act* makes it an offence to fail to take reasonable care of a protected document or protected information, which is suggestive of the language of negligence in indicating an objective standard of care.

Strict liability and absolute liability

3.62 Some criminal offences involve strict liability or absolute liability: that is, these offences do not require any fault elements to be proved. The difference between strict liability and absolute liability is that the defence of an honest and reasonable mistake of fact is available in relation to strict liability offences but not available in relation to absolute liability offences.[60]

3.63 The Senate Standing Committee for the Scrutiny of Bills considered that the requirement of a fault element is one of the most fundamental protections of the criminal law and so strict liability offences only should be introduced after careful consideration and on a case by case basis.[61] In its report, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation*, the Committee suggested that:

> strict liability may be appropriate where it is necessary to ensure the integrity of a regulatory regime such as, for instance, those relating to public health, the environment, or financial or corporate regulation; as with other criteria, however, this should be applied subject to other relevant principles.[62]

3.64 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* notes that 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).[63]

---

59 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 23.

60 *Criminal Code* (Cth) ss 6.1, 6.2. See also *Proudman v Dayman* (1941) 67 CLR 536.

61 Senate Standing Committee for the Scrutiny of Bills, *Application of Absolute and Strict Liability Offences in Commonwealth Legislation* (2002), 283.

62 Ibid, 284.

63 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 24.

3.65 Courts are unlikely to impose strict or absolute liability unless there is a clear and express indication in the legislation.[64] Strict liability offences are relatively common, particularly in the area of regulatory law (such as regulations dealing with safety issues). Absolute liability offences are less common. The ALRC's mapping exercise to date has found a small number of strict liability secrecy offences, including some offences where only part of the physical element of the offence is subject to strict liability.

3.66 Regulation 132(3) of the *Civil Aviation Regulations 1988* (Cth) provides an example of a strict liability secrecy offence:

> (2) An airline, or the owner of an aircraft engaged in public transport service, which uses any air route or airway facility maintained and operated by AA [Airservices Australia] must give CASA [Civil Aviation Safety Authority] or an authorised officer any traffic reports that CASA requires.
>
> (3) A person must not disclose information received under subregulation (2) if the disclosure is not:
>
> (a) in the course of duty to another person performing duties under these regulations;
>
> (b) with the consent of the airline or owner of the aircraft; or
>
> (c) in pursuance of subregulation (4).
>
> (3A) An offence against subregulation (1), (2) or (3) is an offence of strict liability.

3.67 Sometimes strict liability or absolute liability attaches only to one element of the offence. 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.[65] This may include examples where a matter could be peculiarly within the knowledge of the defendant. For example, under s 58 of the *Defence Force Discipline Act 1982* (Cth):

> (1) A person who is a defence member or a defence civilian is guilty of an offence if:
>
> (a) the person discloses information; and
>
> (b) there is no lawful authority for the disclosure; and
>
> (c) the disclosure is likely to be prejudicial to the security or defence of Australia.
>
> Maximum punishment: Imprisonment for 2 years.
>
> (2) Strict liability applies to paragraph (1)(c).

---

64 *He Kaw Teh v R* (1985) 157 CLR 523.

65 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 25.

Note: For strict liability, see section 6.1 of the Criminal Code.

(3) It is a defence if 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.

Note: The defendant bears a legal burden in relation to the matter in subsection (3). See section 13.4 of the Criminal Code.

3.68 In this example, strict liability in relation to paragraph 1(c) is appropriate as it would be very difficult for the prosecution to prove beyond reasonable doubt that the accused thought that the disclosure is likely to be prejudicial to the security or defence of Australia. Rather, the onus is on the accused to prove that he or she neither knew, or could not have been reasonably expected to know, the likely effect of disclosure.

3.69 In ALRC 98, the ALRC considered the introduction of a new summary offence for the act of disclosing classified information. Such an offence would be strict liability, as it would not require the prosecution to establish that the accused had an intention to harm the public interest or that such harm was likely to occur or had occurred as a result of the unauthorised disclosure. It would simply be necessary to prove that the document was classified and that it had been disclosed without authority. The ALRC recommended that the merits of introducing this offence should be considered as part of a broader review of s 79.[66]

3.70 The ALRC is interested in receiving stakeholder views as to the circumstances, if any, in which it might be appropriate for secrecy provisions to contain fault elements other than intent and recklessness.

Question 3–6 In what circumstances might it be appropriate to have fault elements other than intent and recklessness in secrecy provisions?

The public interest

3.71 In ALRC 98, 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.[67] Chapter 2 considers in detail the types of information and which public interests may require protection through secrecy provisions. This chapter considers whether all secrecy provisions should expressly include an element requiring that the unauthorised conduct caused, was likely to cause or intended to cause, some specified harm to the public interest.

66 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–4.

67 Ibid, Rec 5–2.

3.72 Many secrecy provisions do not include an element of this kind. Section 51(2) of the *Australian Crime Commission Act 2002* (Cth), for example, provides:

> (2) 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.

3.73 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 performing duties under the Act. It is not necessary to show that the unauthorised conduct—making a record of, divulging or communicating information—would cause, was likely to cause or was intended to cause any harm to any public interest. These issues might be taken into consideration by the Commonwealth Director of Public Prosecutions in deciding whether to prosecute a person for a breach of the provision, or by the court in deciding on an appropriate penalty for breach of the provision, but they do not form an element of the offence itself.

3.74 By way of contrast, a number of secrecy provisions expressly require that the unauthorised conduct cause, be likely to cause, or be intended to cause harm to a specific public interest. An example of this is s 58 of the *Defence Force Discipline Act*, outlined above. In this provision, the necessary harm to the public interest is expressly stated in that the conduct must be 'likely to be prejudicial to the security or defence of Australia'. Strict liability applies to this element of the offence and so it is not necessary to establish, for example, that the person intended to prejudice the security or defence of Australia, simply that the disclosure was likely to do so.

3.75 Section 79(2) of the *Crimes Act*, on the other hand, requires that a person have the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions.[68]

3.76 Section 193S(3) of the *Aboriginal and Torres Strait Islander Act 2005* (Cth) also expressly requires—as an element of a number of the offences set out in that section—that the conduct would, or would be likely to, harm specific public interests.

---

68 Different penalties apply to breaches of these provisions. The maximum penalty for a breach of s 58 of the *Defence Force Discipline Act* is two years imprisonment. The maximum penalty for a breach of s 79(2) of the *Crimes Act* is seven years imprisonment and a fine of $46,200: see ch 5.

This provision makes it an offence for an Indigenous Land Corporation (ILC) officer to:

> (a) disclose to any person any information concerning the affairs of another person acquired by the ILC officer, where:
>
> (i) the information was acquired by the ILC officer in the performance of duties in connection with an application for, or the giving of, a loan, grant or guarantee; or
>
> (ii) disclosure of the information could reasonably be expected to prejudice substantially the commercial interests of the other person; or
>
> (b) disclose to any person information acquired by the ILC officer, where, to the knowledge of the ILC officer:
>
> (i) the information is considered sacred or otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders; and
>
> (ii) the disclosure would be inconsistent with the views or sensitivities of those Aboriginal persons or Torres Strait Islanders.

3.77 This provision expressly seeks to protect the public interest in safeguarding the commercial interests of persons dealing with the ILC and the public interest in preventing the release of information that is considered sacred or otherwise significant to Aboriginal and Torres Strait Islander people.

3.78 In its final report, the Gibbs Committee considered the need for secrecy offences to include a requirement to prove that the unauthorised disclosure caused some harm and, in this regard, drew a distinction between different categories of protected information. In relation to information relating to defence or foreign relations, for example, the Committee stated that:

> Obviously, the description of information as relating to defence or foreign relations would be so wide that, unless qualified in some way, they would apply to information of an innocuous nature. Thus, no submission disputed that these descriptions needed to be qualified by a requirement to prove harm …[69]

3.79 The Committee recommended that the prosecution should be required to prove harm in relation to a disclosure of information:

- in relation to defence or foreign relations; and
- obtained in confidence from foreign governments and international organisations.[70]

---

69 H Gibbs, R Watson and A Menzies, *Review of Commonwealth Criminal Law: Final Report* (1991), 322.
70 Ibid, 331.

3.80 The Committee recommended that, where proof of damage 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.[71]

3.81 However, in some areas, the Committee considered it was appropriate to impose criminal sanctions without having to establish any harm to the public interest:

> Undoubtedly, a member of the intelligence and security services stands in a special position and it is not unreasonable, in the opinion of the Review Committee, that he or she should be subject to a lifelong duty of secrecy as regards information obtained by virtue of his or her position … the Review Committee is satisfied that disclosures by such persons should be prohibited by criminal sanctions without proof of harm.[72]

3.82 Such an approach is evident in ss 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth), which regulate the Australian Secret Intelligence Service (ASIS), the Defence Imagery and Geospatial Organisation (DIGO) and the Defence Signals Directorate (DSD) respectively. These secrecy provisions bind staff, contractors and others who interact with ASIS, DIGO and the DSD. They create offences for communicating information that was prepared by or on behalf of the organisations, connected with or relating to the performance of the organisations' functions. The provisions do not require that any such disclosure causes, is likely to cause or intended to cause any harm to the public interest.[73]

3.83 Even in the area of national security information, however, not all commentators agree that a blanket prohibition should apply. While McGinness notes that proof of disclosure will generally impose a less onerous burden on the prosecution than proof that disclosure will, or is likely to, cause harm, he expresses the view that:

> One would hope that any reform in Australia, where the process of opening government to public scrutiny is more advanced than in the United Kingdom, would proceed on the basis that a test of harm resulting from disclosure should apply for even the most sensitive categories of national security and defence information.[74]

3.84 McGinness argued that 'it is not sufficient to point to a category of official information that needs protection from unauthorised disclosure'. Rather, he commented:

> Some additional justification is necessary to attract criminal sanctions. Other means are available to protect information outside this special area such as reliance on the loyalty of officials, formal and informal sanctions within a career service and between ministerial colleagues, formal public service disciplinary procedures, security checks

---

71 Ibid, 332. Defences are discussed in Ch 4.

72 Ibid, 323.

73 The text of ss 39, 39A and 40 of the *Intelligence Services Act 2001* (Cth) is set out in Appendix 3.

74 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 77.

> 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*).[75]

3.85 In considering the extent to which government information is protected by, for example, the common law duty of fidelity and good faith or an equitable duty of confidence, the courts have built in a requirement of harm to the public interest.[76] These issues are discussed in Chapter 1.

3.86 An important issue for the ALRC in this Inquiry will be establishing what the concept of 'the public interest' encompasses. In *Sullivan v Farrer*, the High Court noted that:

> the expression 'in the public interest', when used in a statute, classically imports a discretionary value judgement to be made by reference to undefined factual matters, confined only 'in so far as the subject matter and scope and purpose of the statutory enactments may enable … given reasons to be [pronounced] definitely extraneous to any objects the legislature could have had in view'.[77]

3.87 However, judicial opinion differs on how the public interest may be determined. In *McKinnon v Secretary, Department of Treasury*, Hayne J stated that 'it may be readily accepted that most questions about "what is in the public interest" will require consideration of a number of competing arguments about, or features or "facets" of, the public interest'.[78] In contrast, in the same case, Callinan and Heydon JJ took the view that:

> we [are not] by any means certain that it is apt to describe the public interest as multifaceted. Neither the fact that different people will see it differently, nor the fact that an all-encompassing definition of it for all occasions is not possible, means that the public interest is multifaceted.[79]

3.88 In the interests of clarity and certainty, it may be important for secrecy provisions to be explicit about the public interests they are intended to protect. In Chapter 2, the ALRC considers what categories of information warrant the protection of secrecy provisions, including what public interest or interests should be protected by the provisions.[80]

3.89 The ALRC is also interested in stakeholder views on whether, with respect to those categories of information requiring protection, liability should only attach where

---

75 Ibid, 76.

76 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119; *Commonwealth v Fairfax* (1980) 147 CLR 39.

77 *O'Sullivan v Farrer* (1989) 168 CLR 210, 216 (citation omitted).

78 *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, 443.

79 Ibid, 468.

80 See Question 2–5.

the unauthorised conduct causes, is likely to cause or is intended to cause harm to some specified public interest.

Question 3–7 Should all secrecy provisions expressly require that the unauthorised conduct cause, be likely to cause, or be intended to cause harm to a specified public interest?

Constitutional limits

3.90 In ALRC 98, the ALRC recommended that the Australian Government undertake a review of Commonwealth secrecy provisions to ensure that they are consistent with the *Australian Constitution.*[81] This issue arose for consideration by the Federal Court in *Bennett v President, Human Rights and Equal Opportunity Commission*.[82] In that case, Finn J considered reg 7(13) of the *Public Service Regulations*—a predecessor to the current reg 2.1—which stated that:

> An APS employee must not, except in the course of his or her duties as an APS employee or with the Agency Head's express authority, give or disclose, directly or indirectly, any information about public business or anything of which the employee has official knowledge.[83]

3.91 Finn J noted that:

> the only limitations on the information that is caught by the regulation are that information be 'about public business' or that it be 'anything of which the employee has official knowledge'. The former of these limitations would seem to encompass all and any aspect of the structure, conduct and operations of public administration … The reference to 'official knowledge' in the alternative limitation refers to the capacity in which information is derived. If it is derived by a person in his or her official capacity it is caught by the regulation … Neither of the two limitations is, as such, concerned with whether the information in question was or was not otherwise publicly available, or with whether it ought to be or could be made so. Nor are they concerned with whether in a given instance any public interest consideration could reasonably justify a prohibition on disclosure.[84]

3.92 Finn J expressed the view that the regulation was intended to be a 'catch-all' provision, commenting on its 'apparently draconian character' and the possibility that the provision had the potential to produce unreasonable results.[85] He assessed the

---

81 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–5(a).
82 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119.
83 *Public Service Regulations 1999* (Cth) reg 7(13), now repealed and replaced.
84 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119, 133.
85 Ibid, 133.

regulation against the test established in *Lange v Australian Broadcasting Corporation*:[86] first, whether the regulation effectively burdened the implied constitutional freedom of communication about government or political matters; and secondly, if so, whether the regulation was reasonably appropriate and adapted to serve a legitimate end the fulfilment of which was compatible with the maintenance of the system of representative and responsible government prescribed by the *Australian Constitution*. Finn J found that the regulation did burden the implied freedom of political communication, in that it regulated the disclosure by public servants of information about the 'public business' of the Australian Government.

3.93 In relation to the second test, Finn J identified a range of public interests or 'legitimate ends' that would be compatible with maintaining the Australian system of representative and responsible government. These included national security, cabinet confidentiality and the maintenance of an impartial and effective public service. He noted that the 'efficient operation of Government'—a formulation put forward by the Commonwealth in the case—or the 'effective working of Government'—a formulation put forward in the Gibbs Committee's final report—may be legitimate ends but was of the view that the regulation in question was not reasonably and appropriately adapted to those ends. Finn J found that reg 7(13) impaired the implied freedom of political communication in an unnecessary and unreasonable way and, on that basis, that the regulation was inconsistent with the *Australian Constitution* and invalid.

3.94 Finn J stated that:

> Official secrecy has a necessary and proper province in our system of government. A surfeit of secrecy does not. It is unnecessary to enlarge upon why I consider the regulation to be an inefficient provision other than to comment that its ambit is such that even the most scrupulous public servant would find it imposes 'an almost impossible demand' in domestic, social and work related settings …
>
> The dimensions of the control it imposes impedes quite unreasonably the possible flow of information to the community—information which, without possibly prejudicing the interests of the Commonwealth, could only serve to enlarge the public's knowledge and understanding of the operation, practices and policies of executive government.[87]

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

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

87 *Bennett v President, Human Rights and Equal Opportunity Commission* (2003) 204 ALR 119, 141.

and others by unauthorised, improper or premature disclosures of official information.[88]

3.96 He distinguished regulating the disclosure of particular information for legitimate reasons relating to the information or the effects of its disclosure from a 'catch-all' approach, such as that in reg 7(13), which did not differentiate between types of information or the consequences of disclosure. Regulation 7(13) was repealed and has now been replaced by reg 2.1.[89]

3.97 The new regulation was considered by Refshauge J, of the ACT Supreme Court, in *R v Goreng Goreng*.[90] In that case, it was argued that reg 2.1 breached the implied constitutional guarantee of political communication on the basis that prohibiting disclosures that 'could be prejudicial to the effective workings of government' was still too wide and again amounted to a 'catch-all' provision. Refshauge J did not agree. In his view 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—although he noted that 'the effective working of government' did give rise to some indeterminacy requiring the exercise of judgement.[91]

3.98 Richard Jolly has noted that, because secrecy laws specifically target the communication of information about government, such laws may require 'compelling justification' in order to be consistent with the implied freedom of political communication. In discussing the High Court jurisprudence on this issue, he notes the statement by Mason CJ in *Australian Capital Television v Commonwealth*, that in relation to the communication of information or ideas relevant to public affairs:

> only a compelling justification will warrant the imposition of a burden on free communication by way of restriction and the restriction must be no more than is reasonably necessary to achieve the protection of the competing public interest that is invoked to justify the burden on communication.[92]

3.99 Similarly, the Australian Government's *Legislation Handbook* requires that:

> The Attorney-General's Department must be consulted at an early stage on the scope of any new secrecy provisions and on changes to existing secrecy provisions. Secrecy provisions in legislation are to be no broader than is required for the purposes for which they are enacted, particularly bearing in mind the policy underlying the *Freedom of Information Act 1982*.[93]

---

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

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

90 *R v Goreng Goreng* [2008] ACTSC 74.

91 Ibid, [37].

92 *Australian Capital Television Pty Ltd v Commonwealth* (1992) 177 CLR 106, 143.

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

3.100 The ALRC is interested in stakeholder views on whether reg 2.1 of the *Public Service Regulations* provides an appropriate model for protecting Commonwealth information in a way that is consistent with the implied constitutional freedom of political communication. In addition, the ALRC is interested in stakeholder views on whether there are other secrecy provisions that may be inconsistent with the implied freedom. For example, are ss 39, 39A and 40 of the *Intelligence Services Act*, discussed above, consistent with the implied freedom?

Question 3–8 Does reg 2.1 of the *Public Service Regulations 1999* (Cth) provide an appropriate model for protecting Commonwealth information in a way that is consistent with the implied constitutional guarantee of freedom of political communication?

Question 3–9 Are there other secrecy provisions that may be inconsistent with the implied constitutional guarantee of freedom of political communication?

4. Exceptions and Defences

Contents

Introduction

4.1 Commonwealth secrecy laws commonly provide exceptions and defences in relation to the handling of information. Such exceptions and defences may provide, for example, that a Commonwealth officer does not commit an offence, or has a defence, where disclosure of information is made in the course of performing duties under the enactment concerned. This chapter examines how exceptions and defences are formulated in Commonwealth secrecy laws; and asks questions about the exceptions or defences that should apply in future.

4.2 Exceptions and defences in relation to otherwise unauthorised handling of Commonwealth information also may arise under public interest disclosure (or

'whistleblower') legislation. This chapter also discusses existing and possible future public interest disclosure legislation and its relationship with secrecy laws.

'Exception' and 'defence'

4.3 A distinction may be made between exceptions and defences to Commonwealth secrecy laws. This Issues Paper refers to an 'exception' as a provision that limits the scope of conduct prohibited by a secrecy law. A 'defence' is a provision that may be relied on by a person whose conduct is prohibited by a secrecy law. Exceptions are more commonly included in Commonwealth secrecy laws than are defences.

4.4 For example, a secrecy provision in the *Australian Trade Commission Act 1985* (Cth) provides 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.[1] An exception provides that this secrecy provision does not apply to the 'disclosure of information, or the production of a document, to the Minister, to the Secretary to the Department, or to an officer of the Department designated by the Secretary'.[2]

4.5 In comparison, the *Aboriginal and Torres Strait Islander Act 2005* (Cth) provides expressly that 'it is a defence to a prosecution' for divulging 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.[3]

4.6 In some respects, the distinction between an exception and a defence may be of limited significance. In raising either, the defendant faces an evidential burden. At common law, a defence is raised where, in the opinion of the trial judge, sufficient evidence is before the court to make it a genuine issue. In this sense, an evidential burden is placed upon a defendant to raise a defence.[4] 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'.[5] The prosecution must prove all the elements of an offence, positive and negative, and must also disprove any defences raised.[6]

---

1 *Australian Trade Commission Act 1985* (Cth) s 94(2).
2 Ibid s 94(3).
3 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 191(2A).
4 Thomson Legal and Regulatory, *The Laws of Australia*, Evidence, [16.3.4].
5 *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 federal secrecy laws refer to this provision of the *Criminal Code*: see, eg, *Taxation Administration Act 1953* (Cth) s 3(2A); *Building and Construction Industry Improvement Act 2005* (Cth) s 65.
6 Thomson Legal and Regulatory, *The Laws of Australia*, Evidence, [16.3.4].

4.7 While framing a provision as a defence, rather than as an exception, does not alter evidential or legal burdens of proof, it may have procedural disadvantages for a defendant. That is, a defendant will be forced to wait until the defence case is called before being able to lead evidence justifying a disclosure that would otherwise breach a secrecy provision.

General defences

4.8 Some secrecy provisions do not contain any express exception or defence. An example is the secrecy provision applicable to Commonwealth officers contained in the *Crimes Act 1914* (Cth). Section 70(1) states:

> 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.

4.9 Where no exception or defence is expressed, 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.[7]

Summary of existing exceptions and defences

4.10 Most Commonwealth secrecy provisions contain express exceptions or defences relating to prohibited handling of information. These exceptions and defences are formulated in diverse ways. In 1990, John McGinness noted that the impact of so many exceptions, enacted over many years, 'has confused the principles regulating the handling of information within government'.[8]

4.11 The following discussion summarises exceptions and defences currently contained in secrecy laws within a number of broad categories.

Performance of functions and duties

4.12 Secrecy provisions commonly allow information handling in the performance of a person's functions and duties as an employee or officer. Taxation secrecy laws, for example, generally allow information handling in the 'course of duties of an officer'. Secrecy obligations placed on officers by the *Taxation Administration Act 1953* (Cth)

---

7 See *Criminal Code* (Cth); *Criminal Code Act 1995* (Cth) ss 6.1, 9.2.

8 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 61.

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'.[9]

4.13 Similar formulations appear in other areas of Commonwealth legislation. For example:

- the *Racial Discrimination Act 1975* (Cth) provides that secrecy provisions do not prevent the handling of information by a person 'in the performance of a duty under or in connection with this Act';[10]

- the *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) provides that secrecy provisions do not extend to the handling of information by a person 'in the performance of the person's functions or duties' under the Act;[11] and

- the *Disability Services Act 1986* (Cth) provides that secrecy provisions do not apply if a person handles information 'in the performance of duties or exercise of powers' under the Act.[12]

4.14 A 2006 Treasury review of taxation secrecy and disclosure provisions (the Taxation Secrecy Review) stated that the meaning of disclosure in the 'course of duties of an officer' is uncertain and should be clarified.

> Disclosures have not been thought to be allowed in every case where the disclosure would enhance public confidence in the integrity of the tax system. Consequently, it is difficult for officers to be certain about what disclosures are legally authorised.[13]

Required or authorised by law

4.15 Many secrecy provisions incorporate exceptions that specifically allow the handling of information as required or authorised by law. These laws use a range of formulations.

4.16 Secrecy provisions commonly provide that information may be handled 'for the purposes of this Act'. For example:

- the *Taxation Administration Act 1953* (Cth) provides that secrecy provisions do not apply to the handling of information to the extent it is 'for the purposes of this Act';[14]

---

9 *Taxation Administration Act 1953* (Cth) s 3C(2A).
10 *Racial Discrimination Act 1975* (Cth) s 27F(3A).
11 *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2).
12 *Disability Services Act 1986* (Cth) s 28(2A).
13 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 19.
14 *Taxation Administration Act 1953* (Cth) s 3C(2A).

- the *Building and Construction Industry Improvement Act 2005* (Cth) provides an exception to secrecy offences where 'disclosure is for the purposes of this Act';[15] and

- the *Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1988* (Cth) provides that secrecy provisions do not apply if a person is 'acting for the purposes of this Act'.[16]

4.17 It is also common for secrecy provisions to permit disclosure for the purposes of other legislation. For example:

- the *Human Rights and Equal Opportunity Commission Act 1986* (Cth) provides that secrecy provisions do not prohibit a person from handling information as 'required or permitted by an Act … for the purposes of or pursuant to that Act';[17]

- the *Reserve Bank Act 1959* (Cth) provides an exception in relation to disclosure for the purposes of the Act and certain other Acts, including the *Banking Act 1959* (Cth), *Corporations Act 2001* (Cth), *Payment Systems (Regulation) Act 1998* (Cth) and *Payment Systems and Netting Act 1998* (Cth);[18] and

- the *Disability Discrimination Act 1992* (Cth) provides that secrecy provisions do not prohibit the handling of information in accordance with inter-governmental arrangements made under the *Human Rights and Equal Opportunity Commission Act 1986* (Cth).[19]

Authorisation by specified persons

4.18 Some secrecy provisions allow 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'.[20]

4.19 More typically, secrecy provisions permit information handling to be authorised by specified persons—generally the head of an agency or the responsible Minister—provided that other criteria are met. For example:

---

15 *Building and Construction Industry Improvement Act 2005* (Cth) s 65(4).
16 *Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992 (Cth)* s 14(3A).
17 *Human Rights and Equal Opportunity Commission Act 1986* (Cth) s 49(3).
18 *Reserve Bank Act 1959* (Cth) s 79A(2).
19 *Disability Discrimination Act 1992* (Cth) s 127(3).
20 *Superannuation Industry (Supervision) Act 1993* (Cth) s 252C(5)(b).

- 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;[21]

- 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;[22] 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.[23]

Disclosure to specified persons or entities

4.20 Some secrecy provisions provide exceptions where disclosure is made to specified persons or entities, including ministers, Australian Government, state or territory agencies or officials. For example:

- the *Australian Prudential Regulation Authority Act 1998* (Cth) provides exceptions to secrecy provisions where disclosure of information is to the Australian Bureau of Statistics (ABS), the Reserve Bank of Australia, auditors and actuaries;[24]

- the *Industry Research and Development Act 1986* (Cth) provides that secrecy provisions do not apply to the disclosure of information to the Minister, ministerial staff, the Secretary of the Department or a designated officer of the Department;[25] and

- the *Gene Technology Act 2000* (Cth) provides exceptions to secrecy provisions where disclosure is made in the course of carrying out duties or functions under the Act and is to 'the Commonwealth or a Commonwealth authority', a state agency, or the Gene Technology Technical Advisory Committee.[26]

4.21 A particular focus of such exceptions is to authorise information sharing among Australian Government agencies. The *Australian Prudential Regulation Authority Act*, the *Customs Administration Act*, and the *Income Tax Assessment Act 1936* (Cth), for

---

21 *Customs Administration Act 1985* (Cth) s 16(3).
22 *Health Insurance Act 1973* (Cth) s 130(3).
23 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) s 129(1).
24 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(5B), (6A).
25 *Industry Research and Development Act 1986* (Cth) s 47(2).
26 *Gene Technology Act 2000* (Cth) s 187(1)(d).

example, each contain provisions authorising the disclosure of certain information to the ABS.[27]

4.22 In some instances, secrecy provisions permit disclosure in circumstances, or to persons or entities, as prescribed by regulation. For example, the *Medical Indemnity Act 2002* (Cth) allows disclosure of information to a prescribed authority or person.[28] The *Building and Construction Industry Improvement Act 2005* (Cth) provides an exception to disclosure of information offences where disclosure is in accordance with regulations.[29]

Legal proceedings

4.23 Secrecy provisions sometimes provide exceptions expressly permitting the handling of information for the purposes of court or tribunal proceedings. For example:

- the *Fringe Benefits Assessment Act 1986* (Cth) provides that the secrecy provision does not prohibit the Commissioner of Taxation from communicating any information to the Administrative Appeals Tribunal in connection with 'proceedings under an Act of which the Commissioner has the general administration';[30]

- the *Surveillance Devices Act 2004* (Cth) allows information to be handled if it is necessary to do so for purposes of specified criminal and administrative proceedings;[31] and

- the *Pooled Development Funds Act 1992* (Cth) provides that the secrecy provision does not prohibit a person from communicating certain information to 'a court or tribunal in connection with proceedings under this Act or a tax law'.[32]

4.24 Rather than expressly permitting the handling of information for the purposes of court or tribunal proceedings, secrecy provisions more often provide that government office-holders, employees or other persons are not required to disclose information under court or tribunal processes, other than for the purposes of the particular

27 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(5A); *Customs Administration Act 1985* (Cth) s 16(9)(ea); *Income Tax Assessment Act 1936* (Cth) s 16(4)(ga).
28 *Medical Indemnity Act 2002* (Cth) s 77(4).
29 *Building and Construction Industry Improvement Act 2005* (Cth) s 65(4).
30 *Fringe Benefits Tax Assessment Act 1986* (Cth) s 5(5).
31 *Surveillance Devices Act 2004* (Cth) s 45(5).
32 *Pooled Development Funds Act 1992* (Cth) s 71(2).

enactment.[33] As noted in Chapter 1, the extent to which Commonwealth information can be compelled from Commonwealth officers in the course of investigations or in legal proceedings is not a focus of this Inquiry.

Law enforcement purposes

4.25 Commonwealth secrecy laws sometimes provide exceptions expressly permitting the handling of information for various law enforcement and investigatory purposes. These provisions often refer to the investigation of offences. For example:

- the *Crimes Act 1914* (Cth) allows forensic DNA information to be disclosed for the purposes of forensic comparison in the course of a criminal investigation;[34]
- the *Surveillance Devices Act 2004* (Cth) allows information to be handled where necessary to do so for the investigation of certain offences and the making of a decision whether or not to bring a prosecution for an offence;[35] and
- the *Australian Security Intelligence Organisation Act 1979* (Cth) allows the communication of information where the information relates to the commission of an indictable offence.[36]

4.26 Exceptions may extend beyond the investigation of criminal offences 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 investigation by the Privacy Commissioner or Ombudsman; [37]
- the *Child Support (Assessment) Act 1989* (Cth) allows the communication of information about missing and deceased persons where necessary to assist a court, coronial enquiry, Royal Commission, department or authority, of the Commonwealth, a State or a Territory;[38] and
- the *Australian Federal Police Act 1979* (Cth) allows the Commissioner to approve the disclosure of information that relates to the National Witness Protection Program if he or she is of the opinion that it is 'in the interests of the due administration of justice to do so'.[39]

---

33 See, eg, *Australian Security Intelligence Organisation Act 1979* (Cth) s 81(2); *Child Support (Assessment) Act 1989* (Cth) s 150(5); *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32(2).
34 *Crimes Act 1914* (Cth) s 23YO(2).
35 *Surveillance Devices Act 2004* (Cth) s 45(5).
36 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(a).
37 *Crimes Act 1914* (Cth) s 23YO(2).
38 *Child Support (Assessment) Act 1989* (Cth) s 150(4D)–(4F).
39 *Australian Federal Police Act 1979* (Cth) s 60A(2B).

Consent or notice

4.27 Some secrecy provisions provide exceptions permitting the disclosure of information with the consent of the person or entity to whom the information relates or is connected. For example:

- the *Gene Technology Act* permits information to be disclosed 'with the consent of the person who applied to have the information treated as confidential commercial information';[40]
- the *National Health Act 1953* (Cth) provides that certain information about the provision of health services to a patient may be disclosed if the patient consents in writing to the disclosure of the information;[41] and
- the *Reserve Bank Act* states that a person is not prohibited from disclosing information if the person to whose affairs the information or document relates agrees in writing.[42]

4.28 In some instances, where legislation provides exceptions permitting the handling of information, these are subject to further exceptions in relation to the disclosure of personal information, as that term is defined in the *Privacy Act 1988* (Cth).[43] For example, under the *Customs Administration Act* certain authorised disclosures of personal information may take place only where the person to whom the information relates has consented.[44]

4.29 Some secrecy provisions permit disclosure of information after notice and an opportunity to object to disclosure has been provided to certain persons. For example, the *Food Standards Australia New Zealand Act 1991* (Cth) provides that confidential commercial information given by a person may not be disclosed unless the Chief Executive Officer of Food Standards Australia New Zealand has advised the person of this in writing and 'given the person a reasonable opportunity to communicate the person's views about the proposed disclosure of that information'.[45]

---

40 *Gene Technology Act 2000* (Cth) s 187(1)(f).
41 *National Health Act 1953* (Cth) s 135A(8).
42 *Reserve Bank Act 1959* (Cth) s 79A(3).
43 *Privacy Act 1988* (Cth) s 6(1). That is, information 'about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'.
44 *Customs Administration Act 1985* (Cth) s 16(7).
45 *Food Standards Australia New Zealand Act 1991* (Cth) s 114(5).

De-identified information

4.30 Some 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. For example:

- the *Australian Prudential Regulation Authority Act 1998* (Cth) states that it is not an offence if the information disclosed is 'in the form of a summary or collection of information that is prepared so that information relating to any particular person cannot be found out from it';[46]

- the *Census and Statistics Act 1905* (Cth) provides that certain information shall not be 'published or disseminated in a manner that is likely to enable the identification of a particular person or organization';[47] and

- the *Epidemiological Studies (Confidentiality) Act 1981* (Cth) provides that the Act does not prohibit the publication of certain information from prescribed studies 'but such conclusions, statistics or particulars shall not be published in a manner that enables the identification of an individual person'.[48]

Public interest

4.31 A further category of exceptions permits the handling of Commonwealth information in the public or national interest or to avert threats to life or health.

4.32 The *Food Standards Australia New Zealand Act 1991* (Cth), for example, allows the disclosure of certain information if the Minister certifies, by instrument, that it is necessary 'in the public interest'.[49] Similar provisions are found in other statutes, including the *National Health Act 1953* (Cth), *Medical Indemnity Act 2002* (Cth), and *Health Insurance Act 1973* (Cth).[50]

4.33 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'.[51]

---

46 *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(7).
47 *Census and Statistics Act 1905* (Cth) s 12(2).
48 *Epidemiological Studies (Confidentiality) Act 1981* (Cth) s 11.
49 *Food Standards Australia New Zealand Act 1991* (Cth) s 114(4).
50 *National Health Act 1953* (Cth) s 135A(3); *Medical Indemnity Act 2002* (Cth) s 77(3); *Health Insurance Act 1973* (Cth) s 130(3).
51 *Australian Security Intelligence Organisation Act 1979* (Cth) s 18(3)(b).

4.34 Other legislation provides exceptions permitting information to be disclosed in order to avert threats to life or health. For example:

- the *Customs Administration Act* allows the disclosure of information necessary to 'avert or reduce' a 'serious and imminent threat to the health or life of a person';[52]
- 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';[53] and
- the *Child Support (Assessment) Act 1989* (Cth) allows the disclosure of information to prevent or lessen a 'credible threat to the life, health or welfare of a person'.[54]

Absence of harm

4.35 Some secrecy laws prohibit the disclosure of information only where the disclosure is likely to cause harm. Regulation 2.1 of the *Public Service Regulations 1999* (Cth), for example, 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.[55]

4.36 The *Defence Force Discipline Act 1982* (Cth) provides a defence to the offence of unauthorised disclosure of information where 'the person proves that he or she neither knew, nor could reasonably be expected to have known, that the disclosure of the information was likely to be prejudicial to the security or defence of Australia'.[56]

Reform issues

4.37 Possible options for reform in this Inquiry are noted in Chapter 1. The outcomes of this Inquiry may include, for example, recommendations for a new criminal offence of general application to the handling of Commonwealth information; the amendment and consolidation of existing Commonwealth secrecy laws; or model secrecy provisions to assist in drafting future Commonwealth secrecy laws.

---

52 *Customs Administration Act 1985* (Cth) s 16(3F).
53 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34(1A).
54 *Child Support (Assessment) Act 1989* (Cth) s 150(2A)(e).
55 *Public Service Regulations 1999* (Cth) reg 2.1(3). While the regulations do not themselves create a criminal offence, the regulations create a duty of non-disclosure. Breach of this duty may constitute an offence under s 70 of the *Crimes Act 1914* (Cth) or other federal secrecy provision: see Ch 2.
56 *Defence Force Discipline Act 1982* (Cth) s 58(3).

4.38 In this context, the ALRC is interested in comments on the exceptions and defences that should be incorporated into Commonwealth secrecy laws and how existing exceptions and defences may be made more consistent or workable. Aspects of these issues are discussed below.

Exceptions or defences to a general secrecy offence

4.39 The unauthorised handling of Commonwealth information is the subject of a general criminal offence contained in s 70 of the *Crimes Act*.[57] Section 70 does not contain any express exception or defence and, as discussed in Chapter 2, the scope of the offence relies on the existence of a duty not to disclose official information arising under common law, contract, in equity or under separate legislative provisions.[58] As the ALRC asks above: if it is appropriate to retain a general criminal offence for unauthorised handling of Commonwealth information, how should that provision be framed?[59]

4.40 In this context, appropriate exceptions or defences might assist to ensure that a general criminal offence or other specific secrecy provisions are imposed only: (a) in relation to information that genuinely requires protection; (b) where unauthorised disclosure is likely to harm the public interest; and (c) where this is compatible with the maintenance of the system of representative and responsible government prescribed by the *Australian Constitution*.[60]

4.41 For example, a general secrecy law could include requirements that, for an offence to be committed, the person making a disclosure should have reasonable cause to believe that the disclosure would harm certain government interests.

4.42 One model for such a provision is contained in the United Kingdom *Official Secrets Act 1989* (UK). The Act provides for secrecy offences applicable to the disclosure without lawful authority of:

- information relating to security or intelligence, defence or international relations;
- information the disclosure of which could result in the commission of an offence or impede law enforcement;
- information obtained by communications interception or warrant;

---

57 See Ch 2. Other offences are contained in *Crimes Act 1914* (Cth) ss 79 (Official secrets) and *Criminal Code* (Cth) s 91.1 (Offences relating to espionage and similar activities): see App 3.

58 This includes the general duty of an Australian Public Service employee not to disclose official information under *Public Service Regulations 1999* (Cth) reg 2.1.

59 Question 2–1.

60 See Ch 2.

- information resulting from unauthorised disclosures or entrusted in confidence; and

- information entrusted in confidence to other states or international organisations.

4.43 It is an element of most of these offences that the disclosure be 'damaging', as defined in each of the offence provisions. For example, a disclosure of defence-related information is regarded as damaging if:

> (a) it damages the capability of, or of 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; or
>
> (b) otherwise than as mentioned in paragraph (a) above, it endangers the interests of the United Kingdom abroad, seriously obstructs the promotion or protection by the United Kingdom 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.[61]

4.44 It is a defence for a person charged to prove that at the time of the alleged offence he or she did not know, and had no reasonable cause to believe, that the information, document or article in question related to defence or that its disclosure would be damaging.[62]

Question 4–1 If it is appropriate to retain a general criminal offence for unauthorised handling of Commonwealth information, what exceptions or defences should be incorporated in such a provision? For example, should such an offence apply only where the person concerned had reasonable cause to believe that his or her conduct would harm specified public interests? If so, should such a provision be framed as an exception or as a defence?

Consistency of approach to exceptions and defences

4.45 As illustrated in Chapter 2, Commonwealth secrecy laws exhibit a diversity of drafting styles. Existing exceptions and defences also highlight this diversity. While many secrecy laws contain identical or similar exceptions and defences—for example, providing that disclosure of information is not an offence where done in the performance of a person's duties—some provide detailed exceptions that permit disclosure for specified purposes or to specified persons or organisations.

---

61 *Official Secrets Act 1989* (UK) s 2(2)(a).

62 Ibid s 2(3). This defence is not, however, available with respect to the disclosure of information relating to security or intelligence.

4.46 For example, one section of the *Aged Care Act 1997* (Cth) provides 12 detailed exceptions to a prohibition on the disclosure of protected information.[63] Legislation like this, in effect, establishes a code regulating the disclosure of information within and outside government.

4.47 The exceptions and defences provided for by closely related legislation also may vary significantly. It is not always clear that such variation is justifiable. For example, the Taxation Secrecy Review highlighted that various tax secrecy and disclosure provisions can result in different degrees of disclosure to ministers according to the type of tax involved. Information obtained for income tax purposes can be disclosed to a minister where it is in the performance of an officer's duties, but there is an absolute prohibition on the disclosure to ministers of information about indirect taxation, such as information relating to the GST.[64]

4.48 Secrecy provisions applicable to the Australian Securities and Investments Commission and the Australian Prudential Regulation Authority, which operate under similar regulatory legislation, also take different approaches to disclosure to ministers. The *Australian Securities and Investments Commission Act 2001* (Cth) provides that disclosing information to the minister amounts to 'authorised use and disclosure of the information'.[65] The *Australian Prudential Regulation Authority Act* contains no similar exception to its secrecy provisions.

4.49 Another issue concerns the application of secrecy laws to the disclosure of personal information by Commonwealth officers. Some secrecy laws provide exceptions where the disclosure of personal information is with the consent of the person to whom the information relates.[66] Other secrecy laws, such as those relating to officers of the Australian Taxation Office (ATO), do not permit such disclosure.[67] The Taxation Secrecy Review noted that the disclosure of information by the ATO with taxpayer consent would be in line with other secrecy laws.[68]

---

63 The Secretary of the Department may, 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.

64 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 21. See *Income Tax Assessment Act 1936* (Cth) s 16(2), (2A); cf *Taxation Administration Act 1953* (Cth) s 3C(2), (5)(a).

65 *Australian Securities and Investments Commission Act 2001* (Cth) s 127(2A).

66 For example, *Australian Federal Police Act 1979* (Cth) s 60A(2C).

67 *Income Tax Assessment Act 1936* (Cth) s 16.

68 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 27.

4.50 In addition, some secrecy laws provide exceptions where information is already in the public domain. The *Public Service Regulations*, for example, provide an exception to the duty not to disclose information where:

> (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. [69]

4.51 The New South Wales Bar Association has expressed concern that taxation secrecy laws, in contrast, may prevent the ATO from providing professional regulatory bodies with publicly available information, such as the fact that a barrister has been convicted of a taxation offence.[70]

4.52 The Taxation Secrecy Review noted that another source of uncertainty concerns the disclosure of taxation information for the purpose of parliamentary proceedings.[71] The extent to which secrecy laws permit such disclosure, including to parliamentary committees, is sometimes unclear and has been the subject of drafting guidance issued by the Office of Parliamentary Counsel. This is discussed in detail below.

4.53 The ALRC is interested in comments on how exceptions and defences to Commonwealth secrecy laws might be made more consistent. Also, should the exceptions and defences available under secrecy laws be made more consistent with:

- the scope of the equitable action for breach of confidence and the common law employee's duty of fidelity and loyalty (or good faith);[72]
- the general right of access to information provided by the *Freedom of Information Act 1982* (Cth) as limited by the exceptions and exemptions under that Act;[73] or
- regulation of the handling of personal information under the *Privacy Act*?[74]

---

69 *Public Service Regulations 1999* (Cth) reg 2.1(5). See also, for example, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(1) definition of 'protected information' cl (d).

70 New South Wales Bar Association, *Submission to Treasury Review of Taxation Secrecy and Disclosure Provisions*, 26 September 2006.

71 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), 21. See, *Income Tax Assessment Act 1936* (Cth) s 16(2), (2A) cf *Taxation Administration Act 1953* (Cth) s 3C(2), (5)(a).

72 The protection of Commonwealth information by the common law is discussed in Ch 2.

73 The relationship between Commonwealth secrecy laws and freedom of information laws is discussed in Ch 7.

74 The relationship between Commonwealth secrecy laws and privacy law is discussed in Ch 7.

Question 4–2 In what circumstances should Commonwealth secrecy laws permit the disclosure of Commonwealth information:

(a) in the performance of a Commonwealth officer's functions and duties;

(b) as required or authorised by legislation;

(c) on the authority of specified persons;

(d) to ministers or other specified persons or entities;

(e) for the purposes of legal proceedings or law enforcement; or

(f) for other purposes?

Question 4–3 When should provisions in Commonwealth secrecy laws permitting the handling of information generally be framed as exceptions or defences?

Question 4–4 When should Commonwealth secrecy laws include an exception or defence permitting disclosure of personal information, for example, with the consent of the person to whom the information relates or where the personal information is already in the public domain?

Compliance with drafting guidelines

4.54 Some Commonwealth secrecy laws may not comply with current drafting guidelines. For example, the current guide to framing Commonwealth offences provides that:

> The phrases 'without reasonable excuse' or 'section X [being an offence] does not apply if the person has a reasonable excuse' should not be used in the context of Commonwealth offences.[75]

4.55 These phrases are used in at least some secrecy laws. For example, the *Defence Force Discipline Act* provides a defence to the offence of communicating with the

75 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 28. The guide adds that 'these phrases are too open-ended and place uncertainty in the way of any prosecution as to what defence might be raised. Many of the exceptions to criminal responsibility thought to be caught by the "reasonable excuse" defence (such as duress, mistake or ignorance of fact, intervening conduct or event, and lawful authority) are covered by the generic defences in Part 2.3 of the Criminal Code'.

enemy 'if the person proves that he or she had a reasonable excuse for the relevant conduct'.[76]

4.56 Drafting directions issued by Parliamentary Counsel note that secrecy provisions should take into account the possibility that information may be the subject of inquiry by the Parliament or a parliamentary committee—such as under provisions imposing on a parliamentary committee a duty to 'monitor and review' the performance of an authority whose members are subject to a secrecy provision. In such cases, Parliamentary Counsel advises that the secrecy provision should specify the circumstances in which information may be disclosed to the Parliament or parliamentary committee.

> This could be done, in appropriate cases, by including a definition at the end of the secrecy provision to make clear that 'the performance of duties under the Act' includes the giving of evidence to the Parliament or to the specified parliamentary committee.[77]

4.57 The extent to which secrecy laws reflect this advice is unclear. Should this Inquiry, therefore, review the compliance of existing secrecy provisions with current drafting guidelines, such as those issued by the Attorney-General's Department and the Office of Parliamentary Counsel?

Question 4–5 Should the exceptions and defences incorporated in Commonwealth secrecy laws be reviewed to ensure compliance with current drafting guidelines, such as those issued by the Attorney-General's Department and the Office of Parliamentary Counsel?

Public interest disclosure legislation

4.58 Defences to secrecy provisions may be available under public interest disclosure (or 'whistleblower') legislation. Broadly, the objects of public interest disclosure legislation are said to be:

- to support public interest whistleblowing by facilitating disclosure of wrongdoing;
- to ensure that public interest disclosures are properly assessed and, where necessary, investigated and actioned;

76 *Defence Force Discipline Act 1982* (Cth) s 16(2).

77 Parliamentary Counsel, *Drafting Direction No 35: Offences, Penalties, Self-Incrimination, Secrecy Provisions and Enforcement Powers*, Office of Parliamentary Counsel, 13 November 2007, [58]–[62].

- to ensure that a person making a public interest disclosure is protected against detriment and reprisal.[78]

4.59 The 1994 report of the Senate Select Committee on Public Interest Whistleblowing recommended that public interest disclosure should include disclosure of the following categories of wrongdoing:

- illegality, infringement of the law, fraudulent or corrupt conduct;
- substantial misconduct, mismanagement or maladministration, gross or substantial waste of public funds or resources;
- endangering public health or safety, danger to the environment.[79]

State and territory legislation

4.60 All of the states and the ACT have forms of public interest disclosure legislation.[80] This legislation is intended, among other things, to provide protection against offences associated with breaches of state or territory secrecy provisions. For example:

- the *Protected Disclosures Act 1994* (NSW) provides that a person is 'not subject to any liability for making a protected disclosure' and this protection has effect 'despite any duty of secrecy or confidentiality or any other restriction on disclosure (whether or not imposed by an Act) applicable to the person';[81] and

- 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'.[82]

4.61 Public interest disclosure legislation in the other states and the ACT contains similar provisions.[83]

---

78 A Brown, *Whistleblowing in the Australian Public Sector: Enhancing the Theory and Practice of Internal Witness Management in Public Sector Organisations* (2008), 263; Also A Brown, *Public Interest Disclosure Legislation in Australia* (2006) Griffith University, 5.

79 See Australian Parliament—Senate Select Committee on Public Interest Whistleblowing, *In the Public Interest* (1994), 163.

80 *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). A Public Interest Disclosure Bill 2008 (NT) was introduced into the Legislative Assembly on 22 October 2008.

81 *Protected Disclosures Act 1994* (NSW) s 21(1)–(2).

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

83 *Whistleblowers Protection Act 1994* (Qld) s 39(1); *Public Interest Disclosure Act 2003* (WA) s 13; *Whistleblowers Protection Act 1993* (SA) s 5; *Public Interest Disclosures Act 2002* (Tas) s 17; *Public Interest Disclosure Act 1994* (ACT) s 35.

Commonwealth legislation

4.62 A Commonwealth public interest disclosure provision entitled 'Protection for whistleblowers' is set out in the *Public Service Act 1999* (Cth). It provides that a person performing functions for an Australian Government agency 'must not victimise, or discriminate against' an Australian Public Service (APS) employee who has reported breaches of the APS Code of Conduct to the Public Service Commissioner, Merit Protection Commissioner or the head of an agency.[84]

4.63 This public interest disclosure provision is far more limited in its scope than that in the states and territories. Importantly, for present purposes, it does not provide protection against criminal liability under secrecy laws. Dr A J 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.[85]

4.64 This position has been criticised because an APS employee may need to breach the *Public Service Regulations*

> in order to report fraud directly to the AFP, or defective administration to the Ombudsman—even in circumstances where they could not reasonably be expected to first report the conduct within their own agency … Consequently, in the absence of the type of provisions found in other Australian jurisdictions, there are few if any avenues by which Commonwealth officers can make confidential disclosures to outside authorities without facing legal risks.[86]

4.65 Some Commonwealth legislation provides protection in relation to the disclosure of specific types of information, which might be characterised in other contexts as public interest disclosure. For example, the *Aged Care Act*,[87] the *Workplace Relations Act 1996* (Cth)[88] and the *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth)[89] each provide certain persons with protection in relation to specified disclosures, including immunity against 'any civil or criminal liability for making the disclosure'.

---

84 *Public Service Act 1999* (Cth) s 16.
85 A Brown, *Public Interest Disclosure Legislation in Australia* (2006) Griffith University, 34.
86 Ibid, 35. These comments were based on the wording of *Public Service Regulations 1999* (Cth) reg 2.1, prior to amendment in 2006.
87 *Aged Care Act 1997* (Cth) s 96–8.
88 *Workplace Relations Act 1996* (Cth) sch 1, s 337B.
89 *Corporations (Aboriginal and Torres Strait Islander) Act 2006* (Cth) s 469–1.

4.66 More commonly, however, secrecy provisions themselves permit some types of 'public interest disclosure'. For example, the secrecy provision applying to employees of the Australian Federal Police permits disclosure for the purposes of the *Law Enforcement Integrity Commissioner Act 2006* (Cth),[90] under which the Australian Commission for Law Enforcement Integrity investigates whether there has been corrupt conduct by a staff member of a law enforcement agency.[91]

Inquiry into whistleblower protection

4.67 In July 2008, the Australian Government referred the issue of whistleblower protection in the Australian Government public sector to the House of Representatives Standing Committee on Legal and Constitutional Affairs. The Committee is to consider and report on a preferred legislative model to protect public interest disclosures, and is expected to report on the following aspects of its preferred model:

- the categories of people who should be able to make protected disclosures;
- the types of disclosures that should be protected;
- the conditions that should apply to a person making a disclosure;
- the scope of statutory protection that should be available (including immunity from criminal liability and civil penalties);
- procedures in relation to protected disclosures; and
- the relationship between the Committee's preferred model and existing Commonwealth laws.[92]

Relationship with secrecy laws

4.68 Existing state and territory public interest disclosure legislation focuses on the disclosure of information about the improper or corrupt conduct of public officials or public bodies.[93]

4.69 A recent attempt to define public interest disclosure that should be protected at the Commonwealth level is contained in a private member's bill introduced by former Senator Andrew Murray (Australian Democrats). The Public Interest Disclosures Bill 2007 (Cth) provided that 'any public official who discloses public interest information'

---

90 *Australian Federal Police Act 1979* (Cth) s 60A(2)(d).

91 See *Law Enforcement Integrity Commissioner Act 2006* (Cth) s 7.

92 Australian Parliament—House of Representatives Standing Committee on Legal and Constitutional Affairs, *Inquiry into Whistleblowing Protections Within the Australian Government Public Sector: Terms of Reference* (2008) Parliament of Australia. The Committee has been asked to report by February 2009.

93 See, eg, *Protected Disclosures Act 1994* (NSW) s 4 definitions of 'corrupt conduct' and 'public official', s 11 definition of 'maladministration'; *Whistleblowers Protection Act 2001 (Vic)* s 3 definitions of 'corrupt conduct', 'improper conduct' and 'public officer'.

in accordance with the provisions of the bill 'makes a public interest disclosure'.[94] For this purpose, the Bill stated:

> ***public interest information*** means information that shows, tends to show, or that the person providing the information believes on reasonable grounds shows or tends to show, that in relation to the discharge of a Commonwealth public function, a person, authority or corporation has undertaken or proposes to undertake:
>
> (a) improper conduct; or
>
> (b) a serious breach of the Australian Public Service Code of Conduct established by section 13 of the Public Service Act 1999 (other than a breach giving rise only to a private grievance); or
>
> (c) a serious breach of the Parliamentary Service Code of Conduct established by section 13 of the Parliamentary Service Act 1999 (other than a breach giving rise only to a private grievance); or
>
> (d) administrative action that is unjust, discriminatory, unfair or otherwise wrong under the Ombudsman Act 1976; or
>
> (e) action contrary to the Financial Management and Accountability Act 1997; or
>
> (f) abuse of a decision-making power granted under Commonwealth legislation; or
>
> (g) a misuse of public resources (other than an alleged misuse based on mere disagreement over policy that may properly be adopted about amounts, purposes or priorities of expenditure); or
>
> (h) an act or omission that constitutes an offence under a law of the Commonwealth; or
>
> (i) an act or omission that involves a substantial risk of:
>
> (i) injury to a person; or
>
> (ii) prejudice to the security of the Commonwealth; or
>
> (iii) a significant impact on a matter of national environmental significance; or
>
> (j) detrimental action against any person as a result of a public interest disclosure.[95]

4.70 The Bill provides that a public official who makes a public interest disclosure is 'not subject to any civil or criminal liability or any liability arising by way of administrative process (including disciplinary action) for making the disclosure'.[96]

4.71 There is some overlap between public interest disclosure legislation and the exceptions or defences provided under secrecy laws. On the other hand, there are significant differences in relation to the categories of person covered; the types of disclosure covered; and other conditions that must be met before a disclosure is protected or permitted. Some of these differences are illustrated below.

---

94 Public Interest Disclosures Bill 2007 (Cth) cl 7(1).
95 Ibid cl 5.
96 Ibid cl 17.

Categories of person

4.72 Existing state and territory public interest disclosure legislation varies in relation to the categories of person protected. While some legislation applies only to 'public officials',[97] other legislation protects 'any person' who makes a public interest disclosure.[98]

4.73 As discussed in Chapter 3, Commonwealth secrecy provisions vary significantly in relation to the categories of person who are subject to secrecy obligations. Secrecy provisions may extend to regulate the behaviour of persons outside the Australian Government public sector—for example, consultants and others who provide goods and services to the Australian Government.

4.74 Depending on the respective coverage of public interest disclosure legislation and secrecy laws, a person who is subject to a secrecy provision may not be able to obtain protection under public interest disclosure legislation. For example, a person who is an approved provider of aged care services under the *Aged Care Act* is subject to a secrecy provision in that Act.[99] Such a person may not be covered by public interest disclosure legislation that applies only to public sector employees.

Types of disclosure

4.75 There is overlap between the types of disclosure covered by public interest disclosure legislation and exceptions or defences provided under secrecy laws. For example, the Victorian *Whistleblowers Protection Act* extends protection to the disclosure of 'improper conduct', defined to include 'conduct involving substantial risk to public health or safety' that would constitute a criminal offence or reasonable grounds for dismissing a public officer engaged in that conduct.[100] Similarly, some secrecy provisions, such as those in the *Customs Administration Act*, provide exceptions where the disclosure of information is necessary to 'avert or reduce' a 'serious and imminent threat to the health or life of a person'.[101]

4.76 On the other hand, the types of disclosure permitted by exceptions or defences to secrecy laws may be narrower than those protected by public interest disclosure legislation. For example, some public interest disclosure legislation provides protection for the disclosure of information about conduct that would constitute a criminal offence.[102] Secrecy laws also provide exceptions for the disclosure of information relating to the commission of criminal offences but these exceptions may be narrower

---

97 For example, *Protected Disclosures Act 1994* (NSW) s 8.
98 For example, *Whistleblowers Protection Act 2001* (Vic) s 5.
99 *Aged Care Act 1997* (Cth) s 86–2.
100 *Whistleblowers Protection Act 2001* (Vic) s 3.
101 *Customs Administration Act 1985* (Cth) s 16(3F).
102 See, eg, *Protected Disclosures Act 1994* (NSW) s 4 definition of 'corrupt conduct'; *Independent Commission Against Corruption Act 1988* (NSW) s 8(2); *Whistleblowers Protection Act 2001* (Vic) s 3 definition of 'improper conduct'. Also Public Interest Disclosures Bill 2007 (Cth) cl 5, definition of 'public interest information'.

because, for example, disclosure is permitted only for purposes related to the investigation or prosecution of criminal offences.[103]

Conditions on disclosure

4.77 In some respects, however, disclosure protected by public interest disclosure legislation may be more restricted than under exceptions or defences to secrecy provisions.

4.78 The protection extended by public interest disclosure legislation is commonly subject to disclosure being made internally (that is, to a person within the agency concerned) or to a nominated authority, such as an ombudsman. For example, the *Whistleblowers Protection Act 2001* (Vic) provides that a disclosure, in order to be protected, generally must be made to the Ombudsman or, if the disclosure relates to a member, officer or employee of a public body, that public body.[104]

4.79 Exceptions or defences to secrecy law may not be subject to similar conditions—although it is not uncommon for exceptions to provide that disclosure must be made to a specified person, such as the Secretary of a Department or another agency head.[105]

Questions

4.80 The ALRC does not wish to duplicate the deliberations of the House of Representatives Standing Committee on Legal and Constitutional Affairs inquiry into whistleblower protection. The ALRC is interested, however, in comments on the relationship between exceptions and defences provided under Commonwealth secrecy laws and possible new Commonwealth public interest disclosure legislation. For example, should public interest disclosure be incorporated as an exception to criminal offences for unauthorised handling of Commonwealth information?

4.81 Further, should new public interest disclosure legislation, if enacted, exclude disclosure by Commonwealth officers employed by certain agencies—such as those involved in security intelligence or defence? An example of this approach is found in the United Kingdom, where public interest disclosure legislation excludes disclosure by persons employed by intelligence agencies.[106] An alternative approach might permit public interest disclosure only to a specified external agency, such as the Inspector-General of Intelligence and Security.

---

103 See eg, *Customs Administration Act 1985* (Cth) s 16(9).

104 *Whistleblowers Protection Act 2001* (Vic) s 6(1). Other recipient authorities are specified for disclosures that relate to a Member of Parliament, the Chief Commissioner of Police or other members of the police force: *Whistleblowers Protection Act 2001* (Vic) s 6(2), (4)–(5).

105 See, eg *Aged Care Act 1997* (Cth) s 86–3(h).

106 See *Public Interest Disclosure Act 1998* (UK) s 11.

Question 4–6 What should be the relationship between exceptions and defences provided under Commonwealth secrecy laws and possible new Commonwealth public interest disclosure legislation? For example, should public interest disclosure be incorporated as an exception to criminal offences for unauthorised handling of Commonwealth information?

Question 4–7 Should new public interest disclosure legislation, if enacted, exclude disclosure by Commonwealth officers employed by certain agencies—such as those involved in protecting national security?

Question 4–8 Are there other issues in relation to exceptions and defences in Commonwealth secrecy laws that the ALRC should consider in the course of this Inquiry?

5. Penalties

Contents

Introduction

5.1 The existence of penalties can serve a number of purposes, including deterring and punishing unlawful conduct. This chapter addresses the different types of penalties that apply when a secrecy provision is breached. Most secrecy provisions are offences that attract criminal penalties upon breach. Typically, the commission of a secrecy offence will also expose an employee of an Australian Government agency to administrative sanctions. This chapter considers the broader issue of what the consequences of breaching secrecy provisions should be, including when it is appropriate for criminal, civil or administrative penalties to apply. In particular, the chapter considers whether civil penalties should have a greater role to play in addressing unlawful handling of Commonwealth information.

5.2 This chapter highlights inconsistencies in the levels of penalty that apply to secrecy offences and raises questions about the best ways in which a consistent approach to penalties can be achieved. It also considers some issues concerning the drafting of secrecy offences. These include the location of provisions imposing

significant criminal penalties—or imposing duties, the breach of which attracts such penalties—and the lack of clarity about the consequences of breach.

Purpose of penalties

5.3 Penalties for the unauthorised handling of Commonwealth information may serve a number of purposes, depending on the type and level of penalty imposed. These purposes, not all of which may be consistent, can be described as follows:

- to ensure that the offender is punished justly for the offence;
- to deter the offender and others from committing the same or similar offences;
- to promote the rehabilitation of the offender;
- to protect the community by limiting the capacity of the offender to re-offend;
- to denounce the conduct of the offender; and
- to promote the restoration of relations between the community, the offender and the victim.[1]

5.4 The deterrent effect of criminal penalties has been emphasised in a number of other reviews of secrecy laws. For example, in the *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions*, the Treasury expressed the view that 'penalties are required to deter unauthorised disclosure of taxpayer information'.[2] Similarly, the House of Representatives Standing Committee on Legal and Constitutional Affairs has stated that:

> If a penalty is adequate, then it may act as a deterrent to the commission of a crime. Indeed it has been suggested that the worth of the secrecy provisions in the *Crimes Act* is measured by governments not in the number of prosecutions, which are few, but in their deterrence value. However, while prosecutions under the *Crimes Act* are few, this may not indicate the adequacy of the penalty in deterring potential offenders, but rather may be illustrative of the small number of people actually apprehended for those particular offences.[3]

---

1 The ALRC has previously recommended that federal sentencing legislation should provide that a court can impose a sentence on a federal offender only for one or more of the abovementioned purposes: Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006), Rec 4–1.

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

3 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), [5.5.2].

Criminal penalties

5.5 In considering criminal penalties for secrecy offences, it is necessary to examine some principles and legislative provisions that apply in determining penalties for criminal offences generally.

Maximum penalties

5.6 Provisions creating federal offences, including secrecy offences, typically specify the maximum penalty for the offence, which is intended for the worst type of case covered by the offence.[4] Parliament determines the maximum penalties, and courts in sentencing federal offenders are required to determine the sentence or order 'that is of a severity appropriate in all the circumstances of the case'.[5]

5.7 The maximum penalty for an offence is one of the few ways that Parliament can indicate the seriousness of an offence. In *Markarian v The Queen*, the High Court said that:

> Careful attention to maximum penalties will almost always be required, first because the legislature has legislated for them; secondly because they invite comparison between the worst possible case and the case before the court at the time; and thirdly, because in that regard they do provide, taken and balanced with all the other relevant factors, a yardstick.[6]

5.8 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that 'other than in rare cases, Commonwealth offences should carry a maximum penalty rather than a fixed penalty and should not carry a minimum penalty'.[7] Under s 4D of the *Crimes Act 1914* (Cth), the specified penalty for a Commonwealth offence is to be read as being a maximum only, unless the contrary intention appears.

5.9 There are a number of policy reasons why fixed or minimum penalties are generally considered undesirable, including that they:

- interfere with the discretion of a court to impose a penalty appropriate in the circumstances of a particular case;
- preclude the use of available alternative sanctions;

---

4 *Ibbs v The Queen* (1987) 163 CLR 447, 451–452; *Veen v The Queen [No 2]* (1988) 164 CLR 465, 478.

5 *Crimes Act 1914* (Cth) s 16A(1).

6 *Markarian v The Queen* (2005) 215 ALR 213, [31].

7 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 39. The ALRC has previously recommended that no mandatory minimum term of imprisonment is prescribed for any federal offence: Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006), Rec 21–3.

- discourage offenders from cooperating with authorities if such cooperation cannot be taken into account in sentencing; and

- undermine confidence in enforcement where less serious cases do not result in lesser penalties.[8]

Types

5.10 The maximum penalty in provisions creating offences is normally expressed in terms of a monetary fine, penalty units,[9] or a term of imprisonment. In the case of secrecy offences, in the majority of cases, the court has the option of imposing a fine,[10] a term of imprisonment or both. There are, however, a small number of secrecy provisions that specify a fine only.[11]

5.11 Section 17A of the *Crimes Act* reflects the common law position that imprisonment is a sentencing option of last resort.[12] The section provides that a court is not to impose a sentence of imprisonment unless it is satisfied that no other sentence is appropriate in all the circumstances of the case.

5.12 Options apart from fines and imprisonment are available in sentencing federal offenders. Some of these options are expressly set out in Part IB of the *Crimes Act*. Others are picked up from state and territory law by the *Crimes Act* and regulations made under the Act. These are addressed below.[13]

Sentencing options under Part IB of the Crimes Act

5.13 The sentencing options set out in Part IB of the *Crimes Act* include: dismissing the charges;[14] discharging the offender without proceeding to conviction on a finding of guilt;[15] convicting the offender but releasing him or her without passing sentence, on the basis that specified conditions will be complied with;[16] and releasing the offender on recognizance.

---

8 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 40.

9 A penalty unit is defined in the *Crimes Act 1914* (Cth) s 4AA as $110, unless the contrary intention appears.

10 As discussed below, if the offence provision does not specify a maximum fine, there is a formula in Ibid s 4B for calculating the maximum fine that would apply.

11 For example, *Aboriginal and Torres Strait Islander Act 2005* (Cth) s191; *Child Support (Registration and Collection) Act 1988* (Cth) s 58; *Ombudsman Act 1976* (Cth) s 35(2); *Superannuation (Resolution of Complaints) Act 1993* (Cth) s 63(2); *Civil Aviation Regulations 1988* (Cth) reg 132(3).

12 See R Fox and A Freiberg, *Sentencing: State and Federal Law in Victoria* (1999), [9.205]. This approach was endorsed by the ALRC in Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006), [7.145].

13 A detailed examination of sentencing options for federal offenders is discussed in Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006), Ch 7.

14 *Crimes Act 1914* (Cth) s 19B.

15 Ibid s 19B.

16 Ibid s 20(1)(a).

5.14 A recognizance release order involves the court sentencing an offender to a term of imprisonment but ordering that the offender be released, either immediately or after serving a specified period of imprisonment, upon the giving of security that he or she will comply with certain conditions. Security may be given with or without sureties, by recognizance[17] or otherwise.[18] A recognizance release order is essentially a conditional (wholly or partially) suspended sentence of imprisonment.[19]

5.15 The courts have imposed alternative sentencing options on former and current Commonwealth officers found guilty of disclosing Commonwealth information, without authorisation, pursuant to s 70 of the *Crimes Act*. For example:

- In 2007, Allan Kessing, an officer of the Australian Customs Service, was sentenced to imprisonment for a period of nine months but ordered to be released forthwith conditionally upon entering into recognizance in the sum of $1,000 without surety, to be of good behaviour for a period of nine months.[20]

- In 2008, Tjanara Goreng Goreng was convicted and released pursuant to s 20(1)(a) of the *Crimes Act* without passing sentence upon entering in a recognizance in the sum of $2,000, to be of good behaviour for three years and to pay a fine in the sum of $2,000.[21]

Sentencing options under state and territory law

5.16 Section 20AB(1) of the *Crimes Act* provides a mechanism for federal offenders to access a number of sentencing options that are available in the states and territories. The provision specifically identifies some of these sentencing options—for example, community service orders, work orders, attendance centre orders, and sentences of weekend or periodic detention.[22]

5.17 The *Crimes Regulations 1990* (Cth) list other sentencing options available under specified state and territory legislation, such as home detention and intensive correction orders.[23] Some of these options, such as periodic detention, are available only in certain

---

17 A 'recognizance' is an undertaking whereby an offender acknowledges liability to pay a specified amount of money to the Crown unless he or she complies with certain conditions.

18 *Crimes Act 1914* (Cth) s 20(1)(a),(b).

19 The ALRC has previously recommended that the term 'recognizance release order' in the *Crimes Act* should be replaced with terminology that reflects its nature as a conditional suspended sentence: Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006), Rec 2–3.

20 *R v Kessing* [2007] NSWDC 138 [4], [15], [83]. Kessing has appealed his conviction: A Copes, 'Customs Case Back in Court: Whistleblower Fights Conviction', *The Canberra Times*, 3 October 2008, 9.

21 *R v Goreng Goreng* (Unreported, Supreme Court of the Australian Capital Territory, Refshauge J, 14 October 2008).

22 *Crimes Act 1914* (Cth) s 20AB(1) also empowers courts to impose sentencing options that are 'similar' to the ones set out in the provision or listed in the regulations.

23 *Crimes Regulations 1990* (Cth) reg 6.

jurisdictions. Accordingly, when these options are picked up pursuant to s 20AB of the *Crimes Act*, they can only be imposed on federal offenders who are sentenced in the particular jurisdictions in which the options are available.

Application of the *Crimes Act* in determining penalty

5.18 The *Crimes Act* contains a number of provisions relevant to determining the fine that can be imposed on a natural person or corporation for breaching a federal secrecy provision.[24] These provisions are considered below.

Penalty conversions where only sentence of imprisonment specified

5.19 Where an offence provision refers only to imprisonment, ss 4B(2) and 4B(2A) of the *Crimes Act* enable a court to impose a fine if it considers it appropriate to do so. Section 4B(2) sets out a formula to determine the amount of penalty units, being:

> Term of Imprisonment x 5
>
> where:
>
> ***Term of Imprisonment*** is the maximum term of imprisonment, expressed in months, by which the offence is punishable.

5.20 Section 4B(2) of the *Crimes Act* plays a key role in determining the maximum fines that can be imposed for breaches of federal secrecy provisions as a significant number of such provisions are expressed to be punishable by imprisonment only.[25] For example, if a provision specifies a term of imprisonment of two years the applicable fine is 120 penalty units (24 x 5)—amounting to $13,200 (120 x $110). Fines referred to in this chapter have been calculated with reference to s 4B of the *Crimes Act*, where applicable.

5.21 Section 4B(2A) provides that if an offence provides for imprisonment for life, the court may impose a maximum pecuniary penalty of 2,000 penalty units.

Penalty conversion where fine expressed in monetary terms

5.22 A number of secrecy offences specify a maximum fine in dollar terms rather than penalty units.[26] Section 4AB of the *Crimes Act* sets out a formula for converting monetary penalties expressed in dollar amounts to penalty units.[27] This enables fines to take into account changes to the value of a penalty unit. References to fines in this chapter take into account the application of s 4AB, where applicable.

---

24 These provisions are the subject of a general review on criminal penalties by the Attorney-General's Department: *Terms of Reference—Review of Criminal Penalties in Commonwealth Legislation* <http://www.ag.gov.au> at 24 October 2008.

25 Examples of such provisions are discussed below in the section on consistency of penalties.

26 For example, *Australian Institute of Health and Welfare Act 1987* (Cth) s 29 and *Australian Trade Commission Act 1985* (Cth) s 94 each provide for a maximum fine of $2000.

27 For example, if a secrecy provision specifies a fine of $2,000, with the application of *Crimes Act 1914* (Cth) s 4AB, the fine is actually $2200.

Alternate penalties for proceeding summarily on an indictable offence

5.23 Summary offences are those that are either not punishable by imprisonment, or are punishable by imprisonment for a period not exceeding 12 months, unless the contrary intention appears.[28] Indictable federal offences are those that are punishable by imprisonment for a period exceeding 12 months, unless the contrary intention appears.[29]

5.24 Some federal secrecy provisions specify alternate maximum penalties, depending on whether the offence is dealt with summarily or on indictment.[30] The *Crimes Act* provides that certain indictable offences punishable by imprisonment for a period not exceeding 10 years may, unless the contrary intention appears, be dealt with summarily where both the prosecutor and the defendant consent.[31]

5.25 Where a federal secrecy offence is able to be dealt with summarily under the provisions of the *Crimes Act*, the following reduced penalties apply:

- in the case of offences punishable by imprisonment for a period not exceeding five years, the maximum penalty is reduced to a sentence of imprisonment for a period not exceeding 12 months or a fine not exceeding 60 penalty units or both; and

- in the case of offences punishable by imprisonment for a period greater than five years and less than 10 years, the maximum penalty is reduced to a sentence of imprisonment not exceeding two years or a fine not exceeding 120 penalty units or both.

5.26 There are important procedural differences associated with the hearing of indictable and summary offences. Indictable offences are usually tried by a judge sitting with a jury; summary offences by a judge or magistrate sitting alone. Section 80 of the *Australian Constitution* requires that 'the trial on indictment of any offence against the law of the Commonwealth shall be by jury'. The role of a jury in a trial on indictment is to decide the facts of a case and to determine whether or not a defendant is guilty of the offence beyond reasonable doubt. Juries have no role to play in the adjudication of summary offences, or in sentencing.

---

28 Ibid s 4H.
29 Ibid s 4G.
30 Examples of such provisions are discussed below in the section on consistency of penalties.
31 *Crimes Act 1914* (Cth) s 4J. Some secrecy offences such as s 79(2), (5) of the *Crimes Act* cannot be dealt with summarily: Ibid s 4J(7).

Penalties for corporations

5.27 Federal secrecy provisions typically specify the maximum fine or sentence of imprisonment that can be imposed on a natural person. They do not usually specify separate maximum penalties for corporations, although a few provisions do so.[32]

5.28 Many of the sentences that can be imposed on natural persons cannot be imposed on corporations—for example, a corporation cannot be sentenced to imprisonment.[33] Section 4B(3) of the *Crimes Act* empowers a court sentencing a corporation to impose a pecuniary penalty that is up to five times greater than the maximum penalty that could be imposed on a natural person convicted of the same offence, provided that the contrary intention does not appear in the offence provision.

Appropriateness of criminal penalties

5.29 Regulatory theory cautions against the over-use of criminal penalties and looks to gradations of offences matched by a range of penalties. Criminal penalties sit at the top of the 'enforcement pyramid' developed by Professors Ian Ayres and John Braithwaite, to describe an ideal regulatory approach.[34] Under the 'enforcement pyramid' model, breaches of increasing seriousness are dealt with by penalties of increasing severity, with the ultimate penalties—such as imprisonment or loss of a licence to undertake an activity—held in reserve as a threat. Braithwaite has described the operation of the pyramid 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.[35]

5.30 A threshold issue that arises is determining when it is appropriate for criminal penalties to apply when a secrecy provision has been breached. In deciding this issue, regard must be had to a number of factors, including: the effect of a criminal conviction; the need for clarity and certainty in describing conduct to which criminal penalties are to apply; and the public interest in limiting the application of the criminal law to conduct that is deserving of such treatment. For example, is it in the public

---

32 For example, *Sex Discrimination Act 1984* (Cth) s 92, *Defence Act 1903* (Cth) s 73F. This is discussed further below in the section on consistency.

33 The ALRC made a number of recommendations about sentencing options that should be available in sentencing corporations in Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006), Ch 30.

34 The model was first put forward by Braithwaite in J Braithwaite, *To Punish or Persuade: Enforcement of Coal Mine Safety* (1985). See also B Fisse and J Braithwaite, *Corporations, Crime and Accountability* (1993).

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

interest to attach criminal liability to certain conduct currently proscribed by s 79(4)(c) of the *Crimes Act*—that is, a failure to take reasonable care of a protected document or protected information?[36] Would such failure, which is described in negligence terms, more appropriately be dealt with civilly or administratively?

Effect of conviction

5.31 A conviction is a judicial act that alters an offender's legal status.[37] The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* 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'.[38]

5.32 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.[39] A conviction has many consequences beyond the immediate penalty imposed. A person who is convicted of certain offences:

- will be ineligible to hold public office;[40]
- may be ineligible to manage a corporation[41] or be a director or principal executive officer of a company;[42]
- may be required to disclose the fact of his or her criminal conviction in a number of circumstances, for example, in obtaining a drivers' licence or in seeking employment for certain positions;[43] and
- may be deported, if he or she is a non-citizen.[44]

5.33 A convicted offender may lose or be unable to continue in, or obtain, suitable employment—for example, he or she may face deregistration from a professional body. For a public servant, a conviction for an offence involving the unauthorised

---

36 The maximum penalty for breaching *Crimes Act 1914* (Cth) s 79(4)(c) is six months imprisonment and a fine of $3,300.

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

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

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

40 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).

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

42 For example, *Life Insurance Act 1995* (Cth) s 245.

43 This will be subject to the spent conviction provisions in *Crimes Act 1914* (Cth) pt VIIC.

44 For example, *Migration Act 1958* (Cth) s 201.

disclosure of Commonwealth information will most likely result in adverse career prospects or loss of employment, and significant reputational damage.

5.34 A federal offender also may be subject to orders for the confiscation of property in relation to the offence. If a person unlawfully sold Commonwealth information, for example, the proceeds of that sale would be subject to the *Proceeds of Crime Act 2002* (Cth). That Act establishes a scheme to trace, restrain and confiscate the proceeds of crime committed against federal law. The Act aims, among other things, to deprive persons of: the proceeds of offences; the benefits derived from offences; and proceeds derived from the commercial exploitation of their notoriety from having committed offences.[45]

Need for clarity and certainty

5.35 Given the serious consequences of a criminal conviction, it is important that the parameters of conduct that will attract criminal penalties are certain. As a general principle, a person should not be subject to criminal penalties for engaging in ill-defined conduct, the scope of which is ambiguous.

5.36 Chapter 2 discusses the parameters of the offence provision created by s 70 of the *Crimes Act*. Under that provision, a current or former Commonwealth officer who discloses information acquired in the course of duty, being information which it is his or her duty not to disclose, is guilty of an offence punishable by two years imprisonment and $13,200. The duty not to disclose may be one that is found in the common law[46] or in another piece of legislation.

5.37 In his interim report on *Integrity In Government, Official Information*, Paul Finn expressed the view that Commonwealth criminal legislation

> simply attaches criminal sanctions to the breach of whatever secrecy obligation happens to bind a given public official. This, of itself, gives reason for pause. But what makes it particularly obnoxious is that … the secrecy obligations imposed by public service legislation are so all encompassing and unreasonable in their information coverage that strict compliance with them is practically impossible. In their current form those obligations have no place in a modern democratic State. There is an urgent need for their recasting. There is a like need to reconsider what their appropriate relationship should be to the criminal law even after that recasting.[47]

5.38 John McGinness has noted that many secrecy provisions expose officials to penal sanctions for disclosing information, no matter how innocuous, or for disclosing information that already may be public knowledge.[48] McGinness has stated:

---

45 See *Proceeds of Crime Act 2002* (Cth) ss 5, 153. While some forfeiture orders can only be made where a person has been convicted of certain offences, conviction is not always a prerequisite to forfeiture: see Ibid s 48, pt 2–2.

46 The common law duty of fidelity and loyalty is discussed in Ch 1.

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

48 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 72.

> The fact that a prosecution is unlikely to be initiated for disclosure of non-sensitive information is no answer. A person's potential liability to prosecution should be precisely stated in legislation, not left as a matter of discretion to prosecuting authorities. Uncertainty in operation, as the Franks Committee observed, is one of the major faults of official secrets legislation: 'people are not sure what it means or how it operates in practice or what kinds of action involve a real risk of prosecution'.[49]

Which factors should determine whether criminal penalties apply?

5.39 A number of commentators and reports have considered the circumstances in which it is appropriate for criminal penalties to apply when a secrecy provision has been breached. The views expressed focus on varying factors, including: the nature of the information the subject of protection; the intent of the offender; the adverse consequences of a criminal conviction; the seriousness of the breach; and the effect on the public interest if the information were to be disclosed.

5.40 For example, in 1991, in its *Review of Commonwealth Criminal Law*, the Gibbs Committee recommended 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'.[50]

5.41 McGinness has questioned the need for criminal penalties to apply to protect much of the information covered by secrecy provisions, because of the availability of other means of protecting Commonwealth information.

> A large number [of secrecy provisions] can probably be repealed and reliance placed on existing alternative means of protecting sensitive information held by government agencies.[51]

5.42 In 1995, the House of Representatives Standing Committee on Legal and Constitutional Affairs commented on when it is appropriate to invoke criminal penalties for breach of a secrecy provision.

> The application of the criminal law is an appropriate response to the unauthorised disclosure and procurement of confidential third party information in some circumstances. Criminal sanctions are particularly appropriate where information is deliberately released for profit or with malicious intent. However, the criminal law should not operate more widely than is needed as the imposition of criminal sanctions

---

49 Ibid, 73 citing Departmental Committee on s 2 of the *Official Secrets Act 1911* (1972) Vol 1, 14–15 (the 'Franks Committee').

50 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 set out in Ch 2.

51 J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 89.

> can have serious repercussions and may involve deprivation of an individual's liberty[52] …
>
> [The criminal law] should not be invoked unless there is a specific reason for giving certain information special protection … Penal sanctions should be reserved for serious offences where the public interest is best served by imposing those sanctions on the offender.[53]

5.43 In 2006, the Treasury, in reviewing taxation secrecy and disclosure provisions, expressed the view that the use of criminal penalties for the breach of such provisions is more appropriate than the introduction of civil or administrative penalties, because of 'the seriousness with which legislators view such breaches'.[54]

Question 5–1 When should unauthorised handling of Commonwealth information be subject to criminal penalties? Which factors should determine whether or not it is appropriate for criminal penalties to apply?

Consistency

5.44 The Terms of Reference for this Inquiry require the ALRC to consider options for ensuring a consistent approach across government to the protection of Commonwealth information. A significant aspect of consistency of approach must be the consistency of penalties for secrecy offences.

5.45 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* directs those framing offences to 'ensure [the] penalty fits with other penalties in Commonwealth law'.[55]

> 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.[56]

5.46 The Senate Scrutiny of Bills Committee has stated that 'consistency is the main aim of criminal law policy when determining penalties'.[57] Similarly, the House of Representatives Standing Committee on Legal and Constitutional Affairs has

---

52 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), [67].

53 Ibid, [7.2.8].

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

55 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 38.

56 Ibid, 38.

57 Parliament of Australia Senate Scrutiny of Bills Committee, *Scrutiny of Bills Eighth Report of 1998* (1998), [3.8].

expressed the view that 'consistency in the range and expression of penalties in criminal secrecy provisions is desirable,' although 'there may need to be some flexibility depending on the sensitivity of the information to be protected'.[58] More recently, Treasury's *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* recommended that penalties for unauthorised disclosure of protected information should be standardised.[59]

5.47 One way of achieving consistency of penalties is by the articulation of penalty benchmarks for particular categories of offences, to guide those who draft Commonwealth offence provisions.[60]

5.48 There are a number of different ways of assessing consistency of penalties. The discussion below considers consistency of penalties by comparing the penalties:

- in secrecy offence provisions to those which would otherwise apply if formulas in the *Crimes Act* were to apply;
- within secrecy offence provisions that aim to protect similar types of information; and
- for initial and subsequent unauthorised handling of Commonwealth information.

Variations between default fine in s 4B Crimes Act and fines specified in secrecy provisions

5.49 As discussed above, s 4B of the *Crimes Act* stipulates 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. The formula basically adopts a fine/imprisonment ratio of five penalty units to one month of imprisonment (5:1 ratio). Drafting guidelines for Commonwealth offences instruct drafters to adopt the 5:1 ratio 'unless there are grounds to depart from it'.[61]

---

58 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 96–97.

59 The Treasury, *Discussion Paper for the Review of Taxation Secrecy and Disclosure Provisions* (2006), Principle 6.

60 Benchmarks are discussed below in the section dealing with levels of penalty.

61 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 41.

5.50 Where secrecy provisions specify both a maximum fine and imprisonment, the fine to imprisonment ratio is sometimes consistent with the 5:1 ratio in the *Crimes Act*.[62] In other cases the fine to imprisonment ratio in secrecy provisions differs—to varying degrees—from the standard ratio, as illustrated below, in Figure 5.1.

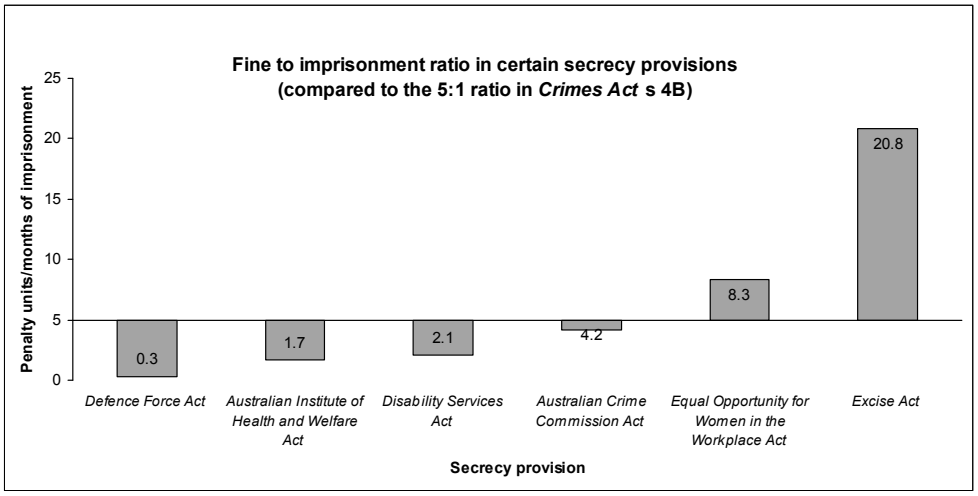

Figure 5.1: Fine/imprisonment ratio shown for the following secrecy provisions: *Defence Force Act 1903* (Cth) s73A (penalty in s 73F); *Australian Institute of Health and Welfare Act 1987* (Cth) s 29; *Disability Services Act 1986* (Cth) s 28; *Australian Crime Commission Act 2002* (Cth) s 51; *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32; *Excise Act 1901* (Cth) s 159.

5.51 Another way of expressing the variations in penalty is to compare the maximum fines that apply under secrecy provisions with the fines that would apply if the formula in s 4B of the *Crimes Act* were adopted. On this analysis, in some cases, the maximum fine stipulated in a secrecy provision is the same as would otherwise apply under the *Crimes Act*.[63] In other cases, the maximum fines stipulated in secrecy provisions range from 15%[64] to more than four times[65] the fines that would otherwise apply under the *Crimes Act*. Within this range fines vary from 33%[66] to approximately 42%[67] to

62 For example, *Intelligence Services Act 2001* (Cth) sch 1 cl 12(1), s 41; *Gene Technology Act 2000* (Cth) s 187(1), s 187(3); *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2), s 23E(4); *Census and Statistics Act 1905* (Cth) s 19(1) and 19(3).

63 For example, *Intelligence Services Act 2001* (Cth) sch 1 cl 12(1), s 41; *Gene Technology Act 2000* (Cth) s 187(1), s 187(3); *Aboriginal Land Rights (Northern Territory) Act 1976* (Cth) s 23E(2), s 23E(4); *Census and Statistics Act 1905* (Cth) ss 19(1), (3).

64 *Defence Act 1903* (Cth) ss 73A, F (where offence dealt with summarily).

65 *Excise Act 1901* (Cth) s 159.

66 *Australian Institute of Health and Welfare Act 1987* (Cth) s 29, *Dairy Produce Act 1986* (Cth) s 119; *Australian Trade Commission Act 1985* (Cth) s 94; *Commonwealth Electoral Act 1918* (Cth) s 323.

67 For example, *Disability Services Act 1986* (Cth) s 28 (where offence dealt with on indictment).

approximately 83%[68] to more than 1.6 times[69] the fines that would otherwise apply under the *Crimes Act*. In at least one case, the fine imposed by the secrecy provision is uncapped.[70]

5.52 There may be valid reasons why a fine stipulated in a secrecy offence varies to this extent from the *Crimes Act* formula. The issue is whether for each of the existing variations there are, in fact, valid reasons to justify the departure. The ALRC is interested in hearing views in this regard.[71]

Variation in corporate multiplier

5.53 As discussed above, under s 4B(3) of the *Crimes Act* the maximum penalty applicable to a body corporate is five times that applicable to a natural person, unless a contrary intention is expressed. Section 73F(2) of the *Defence Act 1903* (Cth) is one example where such a contrary intention is expressed. It prescribes a maximum fine for a body corporate for unlawfully giving or obtaining information about defences of 10 times that which can be imposed on a natural person.[72]

5.54 In an era of decentralised and privatised service delivery, the expanded need for governments to share information with corporations may increase the potential or opportunity for corporations to engage in conduct in breach of a secrecy provision.[73] The ALRC is interested in hearing views about the circumstances in which it may be appropriate for corporations that breach secrecy provisions to be subject to greater or lesser maximum fines than would otherwise apply to them by virtue of the corporate multiplier in the *Crimes Act*.[74]

Variations in penalties for proceeding summarily on an indictable secrecy offence

5.55 The majority of secrecy offences triable on indictment do not specify separate penalties if the offence is dealt with summarily. As discussed above, s 4J of the *Crimes Act* provides that certain indictable offences punishable by imprisonment for a period not exceeding 10 years may, unless the contrary intention appears, be dealt with summarily where both the prosecutor and the defendant consent.

---

68 For example, *Australian Crime Commission Act 2002* (Cth) s 51; *Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992* (Cth) s 14; *Higher Education Funding Act 1988* (Cth) s 78; *Fringe Benefits Tax Assessment Act 1986* (Cth) s 5; *Student Assistance Act 1973* (Cth) s 12ZU; *Taxation Administration Act 1953* (Cth) s 3C(2).

69 For example, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32.

70 *Defence Act 1903* (Cth) s 73A provides that if the offence is dealt with on indictment the maximum penalty is a fine of 'any amount'.

71 See Question 5–2(a) below.

72 The second reading of the Defence Bill 1903 (Cth) does not provide an explanation for this approach: Commonwealth, *Parliamentary Debates*, House of Representatives, 16 July 1903, 2264 (Sir J Forrest), 2275.

73 The principles governing corporate liability are discussed in Ch 3.

74 See Question 5–2(a) below.

5.56 A small number of indictable secrecy provisions indicate a contrary intention to that set out in s 4J of the *Crimes Act*. Examples of such provisions include:

- the *Disability Services Act 1986* (Cth) s 28,[75] and *Telecommunications (Interception and Access) Act 1979* (Cth) s 105,[76] which provide for a maximum term of six months imprisonment on a summary conviction, which is 50% less than would otherwise apply under s 4J of the *Crimes Act*; and

- the *Defence Act* s 73F, which sets out the penalties that are to apply for offences tried summarily and on indictment for a breach of s 73A of the Act.[77] A breach of s 73A, if dealt with on indictment, attracts a maximum penalty of imprisonment 'for any term' or a 'fine of any amount' or both. If the offence is dealt with summarily, the maximum penalty is a $220 fine or imprisonment for six months or both. This provision, unlike s 4J of the *Crimes Act*, allows summary conviction of offences punishable by periods of imprisonment exceeding 10 years.[78]

5.57 There may be valid reasons for a secrecy provision to specify penalties different from those that would apply if the alternate penalties for proceeding summarily on an indictable offence set out in the *Crimes Act* were adopted. In each case, the issue is whether there are, in fact, valid reasons to justify the variation.

5.58 For example, the inconsistency between s 29 of the *Disability Services Act* and s 4J of the *Crimes Act* can be explained by the fact that the *Disability Services Act* predates the addition, in 1987, of s 4J of the *Crimes Act*. In the Second Reading of the Disability Services Bill 1986, Senator Donald Grimes stated that the Bill 'incorporates strict penalties for disclosing information on clients' and that these penalties were a 'further indication that this Bill recognises the rights of people with disabilities'.[79] The Second Reading does not reveal an intention to impose maximum penalties on a summary conviction which are lenient compared to those attaching to the summary convictions of other similar offences.

Variation in distinction between summary and indictable offences

5.59 As noted above, indictable federal offences are those punishable by imprisonment for a period exceeding 12 months, unless the contrary intention

---

75 This provision aims to protect information, acquired in the course of official duties, with respect to the affairs of a person. If tried on indictment it attracts a maximum penalty of two years imprisonment and a fine of $5,500.

76 This provision sets out the penalties on indictment and summary conviction for breaching *Telecommunications (Interception and Access) Act 1979* (Cth) s 63, which protects information obtained by intercepting a communication.

77 Section 73A deals with unlawfully giving or obtaining information as to defences.

78 *Defence Act 1903* (Cth) s 73 is discussed further below in the context of judicial discretion in sentencing.

79 Commonwealth, *Parliamentary Debates*, Senate, 12 November 1986, 1978 (D Grimes).

appears.[80] Offences punishable by imprisonment for a period not exceeding 12 months, or are not punishable by imprisonment, are summary offences unless the contrary intention appears.[81]

5.60 Section 8 of the *Taxation (Interest on Overpayments and Early Payments) Act 1983* (Cth) is an example of a secrecy provision that expresses a contrary intention to the distinction between summary and indictable offences that is set out in the *Crimes Act*. The provision provides for a maximum penalty of two years imprisonment and an $11,000 fine, punishable on summary conviction. This raises the question of when, if ever, it is appropriate for a secrecy provision to specify a maximum penalty imposable on a summary conviction, when an offence carrying that maximum penalty would otherwise be triable before a jury on indictment.

Question 5–2 In what circumstances, if any, is it appropriate for secrecy provisions to specify:

(a) fines for individuals and corporations different from those that would apply if the formulas set out in the *Crimes Act 1914* (Cth) were adopted?

(b) penalties different to those that would apply if the alternate penalties for proceeding summarily on an indictable offence set out in the *Crimes Act* were adopted?

Question 5–3 In what circumstances, if any, is it appropriate for a secrecy provision to specify a penalty punishable on summary conviction when, under the *Crimes Act 1914* (Cth), an offence carrying that maximum penalty would otherwise be tried before a jury on indictment?

Variations in maximum penalty within provisions protecting similar types of information

5.61 The discussion below addresses variations in maximum penalties within provisions protecting similar types of information, namely:

- information relating to the affairs of a person;
- information obtained in the course of duties;
- information relating to law enforcement and investigations;

80 *Crimes Act 1914* (Cth) s 4G.
81 Ibid s 4H.

- defence or security information;
- confidential information; and
- information the disclosure of which is expected to prejudice financial interests.

Information relating to the affairs of a person

5.62 As discussed in Chapter 2, the largest category of secrecy provisions comprises those designed to protect information relating to the affairs of individuals, where that information has been acquired in the course of official duties. Penalties for offences involving the unauthorised acquisition, recording or disclosure of information about the affairs of another person differ widely. A small number of these offences carry a maximum penalty of a fine only, varying, for example, from $550[82] to $1,100[83] to $5,500.[84] The majority, however, are punishable either by a fine or a period of imprisonment, or both. The maximum term of imprisonment for such offences varies from three months[85] to six months[86] to one year[87] to two years,[88] with the majority carrying the latter maximum penalty of imprisonment and, therefore, qualifying as indictable offences.

Information obtained in the course of official duties

5.63 The penalties for breaching secrecy provisions that protect information acquired in the course of official duties vary widely.[89] At least one provision is punishable by a maximum penalty of a fine only, in the amount of $550.[90] The majority, however, are punishable by a term of imprisonment and fine. The maximum term of imprisonment varies from six months[91] to one year[92] to two years,[93] with the majority carrying the latter maximum term of imprisonment and a fine of $13,200. However, there are some

---

82 *Health Insurance Act 1973* (Cth) s 130(1).
83 *Child Support (Registration and Collection) Act 1988* (Cth) s 58.
84 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 191.
85 For example, *Port Statistics Act 1977* (Cth) s 7(1); *Social Welfare Commission (Repeal) Act 1976* (Cth) s 8(1).
86 For example, *Environment Protection (Alligator Rivers Region) Act 1978* (Cth) s 31(2), (4).
87 For example, *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 200A(2) *Australian Institute of Health and Welfare Act 1987* (Cth) s 29; *Sex Discrimination Act 1984* (Cth) s 112; *Racial Discrimination Act 1975* (Cth) s 27F.
88 For example, *A New Tax System (Bonuses for Older Australians) Act 1999* (Cth) s 55; *Aged Care Act 1997* (Cth) s 86-2; *Disability Discrimination Act 1992* (Cth) s 127; *Higher Education Funding Act 1988* (Cth) s 78(4); *Disability Services Act 1986* (Cth) ss 28(2), 29(1); *National Health Act 1953* (Cth) s 135A.
89 The provisions in this category protect any information acquired in the course of duties—not just information relating to the affairs of a person.
90 *Ombudsman Act 1976* (Cth) s 35(2).
91 *Parliamentary Commission of Inquiry (Repeal) Act 1986* (Cth) s 7.
92 *Australian Crime Commission Act 2002* (Cth) s 51.
93 For example, *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34; *Customs Administration Act 1985* (Cth) s 16; *Australian Federal Police Act 1979* (Cth) s 60A; *Australian Security Intelligence Organisation Act 1979* (Cth) s 81; *Trade Practices Act 1974* (Cth) ss 95ZP, 95ZQ.

provisions imposing terms of imprisonment for two years, which attract different maximum fines ranging from $5,500[94] to $11,000.[95]

5.64 One significant example of inconsistency is the penalties that attach to provisions protecting information acquired in the course of performing law enforcement duties.[96] The maximum penalty that applies to members and staff of the Australian Crime Commission (ACC) for recording, divulging or communicating information acquired in the performance of their duties or functions is a term of imprisonment for one year and a $5,500 fine. The maximum penalty applying to members, employees and persons engaged by the Australian Federal Police (AFP) for engaging in similar conduct is two years imprisonment and a fine of $13,200. It is not clear that there is such a significant difference between the nature or sensitivity of the information handled by the ACC and AFP that would justify this disparity.

Information relating to law enforcement and investigations

5.65 There are a variety of secrecy provisions which aim to protect the integrity of the investigation and law enforcement processes. The particular information which is targeted by these provisions varies in its specificity and scope, making it more difficult to draw general conclusions about consistency. Further, some provisions include as an element of the offence the *effect* of the disclosure of information of this type. The maximum terms of imprisonment for offences in this category vary from 10 years[97] to five years[98] to two years[99] to one year,[100] with some offences carrying a maximum penalty of a fine only.[101]

5.66 The highest penalty in this category—10 years imprisonment and a fine of $66,000—attaches to conduct which, among other things, endangers the safety of persons. These include the offences of:

---

94 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 34.

95 *Taxation Administration Act 1953* (Cth) s 13H.

96 Penalties for breach of secrecy provisions protecting information relating to law enforcement and investigations are considered separately below.

97 *Surveillance Devices Act 2004* (Cth) s 45(2); *Witness Protection Act 1994* (Cth) s 22(1).

98 For example, *Witness Protection Act 1994* (Cth) s 22(2) (unauthorised disclosure of information about National Witness Protection Program); *Australian Security Intelligence Organisation Act 1979* (Cth) s 34ZS (unauthorised disclosure of information where questioning and detention warrants have been issued to ASIO for the collection of intelligence on terrorism offences).

99 For example, *Surveillance Devices Act 2004* (Cth) s 45(1) (unauthorised disclosure of information related to an application for a warrant, or emergency or tracking device authorisation); *Telecommunications (Interception and Access) Act 1979* (Cth) ss 63, 105 (unauthorised disclosure of information obtained by intercepting a communication); *Crimes Act 1914* (Cth) s 23YO (unauthorised disclosure of information stored on the Commonwealth DNA database or the National Criminal Investigation DNA database).

100 *Australian Security Intelligence Organisation Act 1979* (Cth) s 92 (disclosure of identity of ASIO employee or agent).

101 For example, *Space Activities Act 1998* (Cth) s 96; *Australian Federal Police Act 1979* (Cth) s 40ZA.

- disclosing information about the identity or location of a person who is or has been a participant in the National Witness Protection Program;[102] and

- publishing information relating to an application for a warrant, an emergency authorisation or a tracking device authorisation, where such conduct endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence.[103]

5.67 In contrast, a person who publishes or otherwise makes public information from which it could reasonably be inferred that another person is a current or former officer, employee or agent of the Australian Security Intelligence Organisation (ASIO), or is in any way connected with a current or former officer, employee or agent of ASIO, is liable to a maximum penalty of imprisonment for one year and a fine of $6,600.[104] In circumstances where such information could endanger the life of an ASIO officer or prejudice the effective conduct of an investigation the maximum penalty appears to be inconsistent with comparable provisions.

5.68 Another example of seemingly inconsistent penalties is found in provisions concerned with investigation records. Under the *Space Activities Act 1998* (Cth), an investigation officer is subject to a maximum fine of $3,300 if he or she discloses a 'safety record' in circumstances other than those set out in the provision. A 'safety record' includes all statements taken in the course of investigation of an accident, and all communications between persons involved in operating a space object that is involved in an accident.[105]

5.69 In contrast, under the *Transport Safety Investigation Act 2003* (Cth) a person who is or has been a staff member is subject to a fine four times that amount—$13,200—as well as imprisonment for two years, if he or she discloses 'restricted information'.[106] Yet, the definition of 'restricted information' is similar to the definition of 'safety record' in the *Space Activities Act*.[107]

Defence or security information

5.70 Not surprisingly, the highest maximum penalties for breach of secrecy provisions are found in provisions that protect defence or security information. The range of maximum penalties varies from imprisonment for 'any term' and a fine of 'any amount' to imprisonment for six months and a fine of $3,300 (on indictment) and a fine of $220 (on summary conviction). Examples of provisions carrying penalties

---

102 See *Witness Protection Act 1994* (Cth) s 22(1).
103 See *Surveillance Devices Act 2004* (Cth) s 45(2).
104 *Australian Security Intelligence Organisation Act 1979* (Cth) s 92.
105 *Space Activities Act 1998* (Cth) s 96.
106 *Transport Safety Investigation Act 2003* (Cth) s 60.
107 It includes all statements obtained in the course of an investigation, and all communication with a person involved in the operation of a transport vehicle that is or was the subject of an investigation: Ibid s 3.

falling within this range are set out below. As these examples demonstrate, the conduct prohibited by these provisions varies widely. In some provisions, the conduct proscribed includes an element that it was undertaken with an intention to prejudice the security or defence of the Commonwealth, or that such prejudice would be likely to result.

5.71 For example, the following range of maximum penalties apply:

- An uncapped term of imprisonment and an uncapped fine for unlawfully communicating or obtaining information relating to any defences of the Commonwealth, if the offence is prosecuted on indictment;[108]
- 25 years imprisonment for various espionage offences;[109]
- 15 years imprisonment where defence members and defence civilians give intelligence to the enemy;[110]
- seven years imprisonment and a fine of $46,200 for:
  - receiving protected information with knowledge that it is communicated in contravention of the espionage offences in s 91.1 of the *Criminal Code* (Cth);[111]
  - communicating, receiving, retaining or allowing unauthorised access to prescribed information, or failing to comply with a lawful direction concerning its retention or disposal, with the intention of prejudicing the security or defence of the Commonwealth;[112] and
  - making, obtaining, collecting, using, possessing, publishing or communicating a document or information relating to an area that has been declared a prohibited area for the purposes of the defence of the Commonwealth;[113]
- two years imprisonment and a fine of $13,200 for:
  - receiving any prescribed document or information with knowledge that the communication is unlawful;[114]

---

108 *Defence Act 1903* (Cth) ss 73A, 73F.
109 See *Criminal Code* (Cth) s 91.1, the text of which is set out in Appendix 3.
110 *Defence Force Discipline Act 1982* (Cth) s 16.
111 *Crimes Act 1914* (Cth) s 79(5).
112 Ibid s 79(2).
113 *Defence (Special Undertakings) Act 1952* (Cth) s 9. See also s 8.
114 *Crimes Act 1914* (Cth), s 79(6).

  - breaching an order made by the Registrar of Designs or the Commissioner of Patents, which respectively prohibits or restricts the publication of information about the subject matter of a design or patent application, in the interests of the defence of the Commonwealth;[115]

- two years imprisonment for unlawfully disclosing information likely to be prejudicial to the security or defence of Australia;[116]

- six months imprisonment and a fine of $3,300 for:

  - retaining a prescribed document when retention is contrary to a person's duty; and

  - failing to take reasonable care of a prescribed document or information;[117] and

- six months imprisonment and a fine of $220 for unlawfully communicating or obtaining information relating to any defences of the Commonwealth, if the offence is prosecuted summarily.[118]

Confidential information

5.72 A number of secrecy provisions aim to protect information that is supplied in confidence, or is confidential in nature. The majority of such provisions, identified by the ALRC to date, are punishable on breach with a maximum penalty of two years imprisonment and a fine of $13,200.[119]

5.73 In comparison, the maximum penalty for the unauthorised disclosure, production, recording or use of any confidential information acquired in the course of duties under the *Equal Opportunity for Women in the Workplace Act 1999* (Cth) is significantly less—imprisonment for three months and a fine of $2,750.

Disclosure of information expected to prejudice financial interests

5.74 Under the *Aboriginal and Torres Strait Islander Act 2005* (Cth), an officer of an Indigenous Land Corporation is subject to a maximum term of imprisonment for one year and a $6,600 fine if he or she discloses information that relates to the affairs of a

---

115 *Designs Act 2003* (Cth) ss 108, 109; *Patents Act 1990* (Cth) s 173.
116 *Defence Force Discipline Act 1982* (Cth) s 58.
117 *Crimes Act 1914* (Cth) s 79(4).
118 *Defence Act 1903* (Cth) ss 73A, 73F.
119 For example, *Gene Technology Act 2000* (Cth) s 187 (confidential commercial information); *Chemical Weapons (Prohibition) Act 1994* (Cth) s 102 (confidential information or documents); *Pooled Development Funds Act 1992* (Cth) s 71 (information supplied in confidence).

person obtained in the course of duties where disclosure could reasonably be expected to prejudice substantially the commercial interests of the person.[120]

5.75 In contrast, under the *Pooled Development Funds Act 1992* (Cth), a person who discloses information 'which may reasonably be expected to affect a person adversely in respect of the lawful business, commercial or financial affairs of the person', is subject to double the above-mentioned maximum penalty—that is, two years imprisonment and a fine in the amount of $13,200.[121]

Consistency of penalties for initial and subsequent unauthorised handling

5.76 Many secrecy provisions apply only to the initial unauthorised handling of Commonwealth information.[122] This is typically an unauthorised disclosure, use or recording by an officer of the relevant agency who possesses the protected information. Other secrecy provisions also seek to regulate the conduct of those persons who have received, pursuant to an authorised disclosure, protected information from a Commonwealth agency or statutory authority. For example, an agency may authorise the release of protected information to a particular recipient on the basis that certain conditions are complied with. If that recipient breaches the conditions on which the information was released, or otherwise unlawfully uses or discloses the protected information, penalties may attach to that subsequent conduct.[123]

5.77 In Chapter 3, the ALRC asks whether all secrecy provisions should seek to regulate initial and subsequent unauthorised handling of Commonwealth information. A related issue that arises is whether penalties should be consistent for both the initial and subsequent unauthorised handling of Commonwealth information. Examples of consistent penalties for initial and subsequent disclosures of protected information can be found in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth)[124] and the *Aged Care Act 1997* (Cth).[125]

Question 5–4 What is the best way to achieve consistency in the maximum criminal penalties for breach of secrecy provisions? Should maximum penalties be referable to the type of information protected, conduct proscribed, fault element; whether or not the conduct harmed the public interest; or a combination of these factors?

---

120 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S.
121 *Pooled Development Funds Act 1992* (Cth) s 71.
122 For example, *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).
123 For example, *Australian Securities and Investments Commission Act 2001* (Cth) s 127(4E), (4EA), (4F).
124 See *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ss 121(2), (7), (12).
125 *Aged Care Act 1997* (Cth) ss 86–2, 86–5.

Question 5–5 If secrecy provisions apply, or are to apply, to both initial and subsequent unauthorised handling of Commonwealth information, should the maximum penalties for initial and subsequent unauthorised handling be consistent?

Level

5.78 Where it is considered appropriate for the criminal law to apply to the breach of a secrecy provision, setting the appropriate level of maximum penalty becomes the next issue.

Penalty benchmarks

5.79 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Power*s states that relevant penalty benchmarks are to be taken into account in setting penalties for offences, and sets out penalty benchmarks for certain classes of offences.[126] 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[127] and subsequent[128] unauthorised handling of Commonwealth information.

5.80 The other benchmarks specified in the interim *Guide* are relevant in gauging the relative criminality of secrecy offences compared with other Commonwealth offences. For example, the interim *Guide* specifies the same penalty benchmarks for breaching confidentiality requirements and for making false statements in applications for warrants.[129] It also sets out the following benchmarks:

- six months imprisonment or 30 penalty units for offences by witnesses;
- 50 to 60 penalty units for failure to lodge reports or returns;
- 12 months imprisonment or 60 penalty units for making false statements in notices or applications or failing to provide information that is required;
- five years imprisonment or 300 penalty units for corruption and abuse of public office; and

126 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 47.
127 *Data-matching Program (Assistance and Tax) Act 1990* (Cth) s 15; *Customs Administration Act 1985* (Cth) s 16(2).
128 *Australian Hearing Services Act 1991* (Cth) s 67(8).
129 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 47.

- life imprisonment for treason, certain war crimes and terrorist acts.[130]

5.81 The ALRC is interested in hearing views about whether the current penalty benchmark for breach of secrecy offences is adequate to cover the full spectrum of secrecy offences, or whether there is a need to have a broader spectrum of penalty benchmarks depending on how secrecy offences are to be categorised.

Comparing penalties across different types of protected information

5.82 In assessing what levels of penalty should apply to particular secrecy offences, there is scope for comparing levels of penalty to proscribed conduct *across* different types of protected information. A value judgement about the comparative importance of protecting different types of information may be implicit in the levels of maximum penalties attached to the unauthorised handling of those types of information.

5.83 For example, under the *Aboriginal and Torres Strait Islander Act 2005* (Cth) an officer of an Indigenous Land Corporation is subject to a maximum term of imprisonment for one year and a $6,600 fine if he or she discloses information that is considered sacred or otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders; and the disclosure would be inconsistent with the views or sensitivities of those persons.[131] In contrast, as discussed above, the usual maximum penalty for disclosing confidential information is double that level—two years imprisonment and a fine of $13,200. In addition, the maximum penalty attaching to the unauthorised disclosure of information expected to affect adversely a person's financial affairs[132] in some cases is greater than the penalty attaching to the unauthorised disclosure of sacred information. This raises the issue of whether such a discrepancy is appropriate.

5.84 Further, is it appropriate that the maximum term of imprisonment for the offences of disclosing information likely to prejudice the defence or security of Australia[133] or breaching orders made in the interests of the defence of Australia[134] is the same as those attaching to many offences concerning the disclosure of information related to the affairs of a person?[135]

---

130 Ibid, 47–48.

131 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S.

132 For example *Pooled Development Funds Act 1992* (Cth) s 71 (two years imprisonment and fine of $13, 200).

133 *Defence Force Discipline Act 1982* (Cth) s 58 (two years imprisonment). Strict liability applies to the element that the disclosure is likely to be prejudicial to the defence or security of Australia: s 58(2).

134 *Designs Act 2003* (Cth) ss 108, 109; *Patents Act 1990* (Cth) s 173.

135 For example, *Taxation Administration Act 1953* (Cth) s 3C(2).

Role of judicial discretion and interaction with maximum penalty

5.85 Both the Australian Parliament in setting maximum penalties for offences, and sentencing courts in determining the actual penalty to be imposed in a particular case, play an important part in endeavouring to ensure that an appropriate type and level of penalty is imposed on an offender.

5.86 In sentencing a federal offender, s 16A(2) of the *Crimes Act* requires a court to take into account specified factors, to the extent that they are relevant and known. Among the factors that are to be considered are the 'nature and circumstances of the offence' and 'any injury, loss or damage resulting from the offence'. Each of these factors is addressed below.

5.87 The 'nature and circumstances' of the offence would entail a consideration, for example, of: the sensitivity of the information the subject of unauthorised conduct (for example, whether it was national security information); the type of conduct proscribed (for example, disclosure or mere receipt); and whether the conduct was intentional.[136]

5.88 The factor of 'any injury, loss or damage resulting from the offence' would entail a consideration of the consequences of breaching a secrecy provision; for example, whether the breach endangered life or safety, or prejudiced national security, an investigation, or a person's financial interests. Many secrecy offences do not contain an element of a likelihood of harm to an identifiable public interest. For such offences, the prosecution does not need to prove beyond reasonable doubt that harm did or was likely to ensue in order to establish criminal liability. However, where the conduct, in fact, harms the public interest, the fact and degree of harm are relevant aggravating factors to be considered in sentencing.

5.89 Some secrecy provisions, however, contain as an element of the offence to be proved that the unauthorised handling of Commonwealth information risked, or caused, harm to an identifiable public interest. The *degree* of harm to the public interest would be a relevant factor in sentencing.

5.90 The question arises whether the maximum level of penalty determined by Parliament to attach to secrecy offences which contain an element of likelihood of damage to an identifiable public interest should be higher than secrecy offences that do not contain such an element. Such an approach is taken in the *Surveillance Act 2004* (Cth) s 45(1), which provides a maximum penalty of two years imprisonment and a fine of $13,200 for the unauthorised use, recording or disclosure of protected information. Section 45(2) provides a maximum penalty of 10 years imprisonment and a fine of $66,000—a fivefold increase—where the same unauthorised conduct 'endangers the health or safety of any person or prejudices the effective conduct of an investigation into a relevant offence'.

---

136 Such factors may also influence the determination by the Australian Parliament of the level of maximum penalty that should apply to secrecy offences. The ALRC asks above about the extent to which maximum penalties should be referable to such factors: see Question 5–4.

Complete judicial discretion

5.91 As noted above, s 73F of the *Defence Act 1903* is anomalous in that it allows a judge unfettered discretion with respect to the level of penalty that may be imposed for breach of the secrecy provision in s 73A of the Act, when dealt with on indictment. The *Defence Act 1903* is an old Act, which may not always conform with modern drafting guidelines. Breach of s 73A attracts a maximum penalty of imprisonment 'for any term' or a 'fine of any amount' or both. The breadth of the sentencing possibilities under this provision is extensive—encompassing both lenient and punitive outcomes. For example, a judge could impose a fine of $550 only, or a term of life imprisonment. This raises the issue of whether it is ever appropriate to give a sentencing court complete discretion as to the maximum penalty to be imposed for a secrecy offence.

Short sentences of imprisonment

5.92 A number of secrecy provisions specify maximum terms of imprisonment of three months.[137] This raises the issue of whether short sentences of imprisonment can be appropriate for breach of secrecy provisions.

5.93 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* directs those framing Commonwealth offences to refrain from imposing terms of imprisonment of less than six months. It states that:

> Avoiding provision for short term prison terms underlines the message that imprisonment is reserved for serious offences and also avoids the potential for burdening State/Territory correctional systems with minor offenders.[138]

5.94 In contrast, in *Same Crime, Same Time: Sentencing of Federal Offenders*, the ALRC recommended that sentences of imprisonment of less than six months should continue to be available in the sentencing of federal offenders.[139] The ALRC expressed the view that the federal sentencing regime protects against the inappropriate imposition of short sentences.[140] The ALRC noted that anecdotal evidence from Western Australia indicates that the abolition of short sentences may have perverse consequences, resulting in offenders receiving longer sentences of imprisonment than would otherwise have been warranted.[141]

---

137 See, eg, *Equal Opportunity for Women in the Workplace Act 1999* (Cth) s 32; *Port Statistics Act 1977* (Cth) s 7; *Defence (Inquiry) Regulations 1985* (Cth) reg 63.

138 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 42–43.

139 Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006) Rec 7–8.

140 As noted above, *Crimes Act 1914* (Cth) s 17A provides that a sentence of imprisonment should not be imposed for a federal offence unless the court is satisfied that no other sentence is appropriate in the circumstances of the case.

141 See Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006) [7.70]–[7.72].

Question 5–6 Should there be benchmarks for the maximum levels of criminal penalties that apply to secrecy offences according to their categorisation? If so, what should those benchmarks be? For example, should the maximum level of penalty that attaches to offences involving:

(a) the unauthorised handling of national security information; or

(b) an element of likelihood of harm to the public interest

carry higher maximum criminal penalties than those that do not?

Question 5–7 Are there any circumstances in which it is appropriate for a secrecy provision to give a sentencing court complete discretion as to the maximum level of penalty that is to apply (as is the case in the secrecy provision in the *Defence Act 1903* (Cth))?

Drafting issues

5.95 A number of drafting issues are raised by some secrecy provisions, including: the location of provisions imposing significant criminal penalties or imposing duties, the breach of which attract such penalties; the lack of clarity of consequences attaching to breach; and the fact that some provisions express maximum fines in dollar terms.

Location

5.96 Locating criminal offences and penalties in primary legislation increases their visibility and scrutiny by the Australian Parliament. This approach is confirmed in the interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers*, which states that:

> It has long been the approach of the Commonwealth Parliament and Commonwealth Governments that serious criminal offences and penalties should be contained in Acts of Parliament rather than subordinate legislation, irrespective of the penalty to be imposed. It is important that serious offences pass through the full Parliamentary process, so that the Parliament can give close attention to the scope of the offence and the appropriateness of the penalty. There is also a legitimate expectation on the part of those who read legislation that fundamental aspects of a legislative scheme (such as serious criminal offences) will be contained in the parent Act.[142]

5.97 The majority of secrecy offences are contained in primary legislation. However, a number of Commonwealth regulations contain secrecy offences to which penalties of fines and imprisonment attach.

---

142 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 43.

5.98 The *Legislation Handbook* (1999) provides guidance on the types of matters that should be included in primary and subordinate legislation, respectively.[143] The *Handbook* states that provisions creating offences which impose significant criminal penalties should be implemented only through Acts of Parliament. It defines significant criminal penalties as 'imprisonment or fines equal to more than 10 penalty units for individuals or more than 50 penalty units for corporations'.[144]

5.99 The more recent (2007) interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* expresses a different opinion about the maximum fine that is appropriate to be included in a regulation for breach of an offence. It provides that regulations should only specify fines which do not exceed 50 penalty units for natural persons and 250 penalty units for a body corporate.[145]

5.100 There are a small number of secrecy offences contained in regulations that impose terms of imprisonment,[146] raising the question whether these offences should be relocated to the relevant primary legislation.

5.101 There are also regulations which impose a duty of non-disclosure, a breach of which is subject to a maximum penalty of two years imprisonment and fine of $13,200 under s 70 of the *Crimes Act*. This applies, for example, to a breach of *Public Service Regulations 1999* (Cth) reg 2.1—which expressly refers to the application of s 70 of the *Crimes Act*. It may also apply to a breach of *Commonwealth Inscribed Stock Regulations (Statutory Rules 1944)* (Cth) reg 61, which provides that an officer of a Registry for the inscription of stock must not divulge information obtained in the course of duties except in specified circumstances.[147]

5.102 Can it be appropriate for a duty of non-disclosure to be set out in a regulation, where breach of that duty attracts—by virtue of the application of another provision—a significant criminal penalty?

Clarity regarding consequences of breach

5.103 The consequences of breach of a secrecy provision should be clear and unambiguous. In circumstances where a criminal penalty applies, the need for clarity in the interests of fairness is paramount. The potential liability for breaching secrecy provisions is not always readily apparent, however.

---

143 The *Legislation Handbook* is intended as a guide for departmental officers involved in the development of legislation: Department of Prime Minister and Cabinet, *Legislation Handbook* (1999), 1.

144 Ibid, 3.

145 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 43.

146 For example, *Defence (Inquiry) Regulations 1985* (Cth) regs 62, 63 each specify a maximum penalty of five penalty units or imprisonment for three months.

147 This regulation does not refer to the application of *Crimes Act 1914* (Cth) s 70. The need for clarity as to the consequences of breach of a secrecy provision is addressed below.

5.104 Under s 70 of the *Crimes Act*, whenever an existing or former Commonwealth officer discloses information acquired in the course of being a Commonwealth officer, and which it is or was his or her duty not to disclose, the officer is guilty of an offence punishable by two years imprisonment, and a fine of $13,200. A duty not to disclose may be set out in another statutory provision. In such circumstances, the issue arises whether the provision setting out the duty of non-disclosure should refer expressly to liability attaching under s 70 of the *Crimes Act*. This would alert an officer to the maximum penalty and remove any ambiguity about whether or not criminal liability attaches.

5.105 Section 30A of the *Archives Act 1983* (Cth) provides an example of a provision which sets out a duty of non-disclosure and makes express reference to the application of s 70 of the *Crimes Act* for breaching this duty.[148] Other secrecy provisions do not refer to the consequences of breach. For example, s 114(1) of the *Food Standards Australia New Zealand Act 1991* (Cth) sets out the duty of officers not to disclose confidential commercial information acquired in the course of functions, but does not specify a penalty for breaching this duty. Presumably s 70 of the *Crimes Act* applies, but its application is not readily apparent.[149]

5.106 Other examples of secrecy provisions where the consequences of breach are not clear and where the question of the applicability of s 70 of the *Crimes Act* arises, include:

- s 127 of the *Australian Securities and Investments Commission Act 2001* (Cth), which provides that ASIC must take all reasonable measures to protect from unauthorised use or disclosure protected information and information obtained in the performance of its functions or obtained in confidence;[150] and

- s 47 of the *Industry Research and Development Fund Act 1986* (Cth), which states that relevant officials must not, except in defined circumstances, supply protected information to a person if it would constitute a breach of confidence.[151]

Reference to penalty units

5.107 Drafting guidelines for Commonwealth legislation state that, as a general drafting principle, fines should be expressed in penalty units to assist in adjusting

148 See also *Public Service Regulations 1999* (Cth) reg 2.1.

149 The provision does, however, specify a maximum penalty of two years imprisonment in circumstances where an unauthorised secondary 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.

150 The section only specifies penalties in respect of conduct engaged in by those to whom ASIC discloses such information: *Australian Securities and Investments Commission Act 2001* (Cth) s 127(4E), (4EA).

151 See also *Australian Security Intelligence Organisation Act 1979* (Cth) s 40; *Migration Act 1958* (Cth) s 503A.

penalties upwards in line with inflation.[152] The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that:

> There may be limited circumstances where the use of dollar penalties is more appropriate; for example, where an existing scheme already uses dollar amounts.
>
> At present, a penalty unit equals $110 … (*Crimes Act*, section 4AA). However, when the value of a penalty unit is increased by amending s 4AA, the increase also applies to penalties expressed in dollar amounts via section 4AB.[153]

5.108 Many secrecy offences express the maximum fine in dollar amounts.[154] Should these offence provisions be redrafted to refer expressly to the maximum number of penalty units, or is this unnecessary because of the application of s 4AB of the *Crimes Act*?[155]

Question 5–8 Given conflicting drafting guidelines about what level of fine amounts to a significant criminal penalty—which should therefore only attach to offences in primary legislation—what is an appropriate maximum level of fine for a secrecy offence that is located in a regulation?

Question 5–9 Should those secrecy offence provisions that are currently located in regulations and which either:

(a) carry a term of imprisonment or a significant fine; or

(b) specify a duty of non-disclosure which attracts a term of imprisonment because of the application of s 70 of the *Crimes Act 1914* (Cth)

be relocated to primary legislation?

Question 5–10 Should all secrecy provisions be drafted to ensure that the consequences of breach are clear on their face? For example, if the penalty for breaching a duty of non-disclosure set out in a secrecy provision is set out in another legislative provision (such as s 70 of the *Crimes Act 1914* (Cth)) should the secrecy provision cross-refer expressly to the other legislative provision?

---

152 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 44.

153 Ibid, 44.

154 For example, *Australian Institute of Health and Welfare Act 1987* (Cth) s 29 ($2,000); *Child Support (Registration and Collection) Act 1988* (Cth) s58 ($1,000); *Australian Trade Commission Act 1985* (Cth) ($2,000); *Environment Protection (Alligator Rivers Region) Act 1978* (Cth) s 31(2), (4) ($1,000).

155 The conversion formula in *Crimes Act 1914* (Cth) s 4AB is discussed above.

Question 5–11 Is there a need to redraft those secrecy offence provisions that refer to maximum fines in monetary terms rather than penalty units or is this unnecessary because of the application of s 4AB of the *Crimes Act 1914* (Cth)?

Administrative penalties

5.109 Broadly, administrative penalties include those which arise automatically by operation of legislation, as well as those which can be imposed directly by an agency or regulator. This distinguishes them from criminal and civil penalties, which only may be imposed by courts.[156]

5.110 Under Chapter III of the *Australian Constitution*, non-judicial officers are precluded from exercising the judicial power of the Commonwealth. This means that such officers cannot impose a fine[157] or impose punishment for an offence.[158] The basis for this approach is the doctrine of the separation of powers.

Types

5.111 Commonwealth officers are subject to a range of administrative penalties and actions for breaching secrecy provisions, from reprimands and counselling to dismissal from employment. While reprimands and counselling may be at the base of the 'enforcement pyramid' developed by Ayres and Braithwaite, dismissal from employment is more severe and positioned higher up the pyramid (but short of imprisonment).

5.112 Commonwealth officers employed under the *Public Service Act 1999* (Cth) are subject to a range of administrative penalties for breaching secrecy provisions. These penalties are outlined below. Many Commonwealth officers who potentially handle the most sensitive Commonwealth information, however, fall outside the ambit of the *Public Service Act*. These include employees and members of the Australian Defence Force (ADF), the cadet force, the AFP, the Australian Security Intelligence Organisation (ASIO) and the Australian Security Intelligence Service (ASIS). The discussion below outlines the administrative penalties available against persons in the ADF, cadet force and AFP.

5.113 The constituting legislation of ASIO and ASIS does not set out administrative penalties for breach of secrecy provisions. Terms and conditions of employment of staff of ASIO and ASIS are determined, respectively, by the Directors-General of

---

156 As discussed below, however, the Australian Military Court (which is not a court for the purposes of Ch III of the *Australian Constitution*) has the power to impose certain administrative penalties following a conviction.

157 *R v White; Ex Parte Byrnes* (1963) 109 CLR 665, 669–670.

158 *Federal Commissioner of Taxation v Munro* (1926) 38 CLR 153, 175.

Security and of ASIS.[159] The ALRC is interested in hearing about the types of administrative penalties applicable to ASIO and ASIS officers, and whether they are adequate and appropriate. The ALRC is also interested in hearing whether the administrative penalties available under the legislative schemes discussed below are adequate and appropriate.

Penalties under Public Service Act 1999 (Cth)

5.114 Section 13 of the *Public Service Act* sets out the Australian Public Service (APS) Code of Conduct, which binds APS employees, the secretary of a department, the head of an executive agency or statutory agency, and statutory officeholders.[160] 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;
- maintain appropriate confidentiality about dealings that the employee has with any minister or minister's member of staff; and
- comply with any other conduct requirement that is prescribed in the regulations.[161]

5.115 Where an APS employee breaches the 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, by way of fine, which is not to exceed 2% of the APS employee's annual salary;[162] and a reprimand.[163]

5.116 The *Public Service Regulations 1999* (Cth) provide that an agency head may suspend an APS employee from duties if the agency head believes on reasonable grounds that the employee has, or may have, breached the Code of Conduct, and

---

159 *Australian Security Intelligence Organisation Act 1979* (Cth) ss 86, 89; *Intelligence Services Act 2001* (Cth) s 33. See also Ch 6.

160 See *Public Service Act 1999* (Cth) ss 7, 14.

161 *Public Service Regulations 1999* (Cth) reg 2.1, discussed in Ch 3, sets out the circumstances in which an APS employee is precluded from disclosing Commonwealth information.

162 *Public Service Act 1999* (Cth) s 15; *Public Service Regulations 1999* (Cth) reg 2.3. Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 85 opposed an increase in the maximum fine payable under the *Public Service Act* on the basis that 'it would make the fine more akin to a criminal penalty than an administrative sanction'.

163 *Public Service Act 1999* (Cth) s 15. The processes for investigating, determining, and reviewing findings of breach of the Code of Conduct are discussed in Ch 6.

suspension is in the public or the agency's interest. The regulations also provide that an agency head:

- may decide whether the suspension is with or without remuneration;[164] and
- must immediately end the suspension if a penalty has been imposed on the APS employee for the relevant breach of the Code of Conduct.[165]

5.117 Because an APS employee who commits a secrecy offence automatically breaches the APS Code of Conduct, he or she will be liable to both criminal and administrative penalties for the same conduct.

Penalties under Defence Force Discipline Act 1982 (Cth)

5.118 There are two secrecy provisions in the *Defence Force Discipline Act* (DFD Act). Section 16 prohibits communicating with, or giving intelligence to, the enemy and is punishable by 15 years imprisonment. Section 58 prohibits the unlawful disclosure of information likely to be prejudicial to the defence or security of Australia, and is punishable by two years imprisonment.

5.119 Section 68(1) of the DFD Act sets out the only punishments that may be imposed by a service tribunal on a convicted person.[166] These punishments, in decreasing order of severity, are:

(a) imprisonment for life;

(b) imprisonment for a specific period;

(c) dismissal from the Defence Force;

(d) detention for a period not exceeding two years; [167]

(e) reduction in rank;

(f) forfeiture of service for the purposes of promotion;

(g) forfeiture of seniority;

(h) fine, being a fine not exceeding:

i) where the convicted person is a member of the Defence Force—the amount of his or her pay for 28 days; or

ii) in any other case—$500;

---

164 The maximum period of suspension without remuneration is 30 days unless exceptional circumstances apply: *Public Service Regulations 1999* (Cth) reg 3.10(2), (3).

165 Ibid reg 3.10(6).

166 A service tribunal is defined as the Australian Military Court or a summary authority. A summary authority comprises members of the ADF and includes a superior summary authority, a commanding officer or a subordinate summary authority: see *Defence Force Discipline Act 1982* (Cth) ss 3(1), 105, 114.

167 A detention centre is defined as 'a place, not being a prison, that is operated by the [ADF] as a place for the detention of persons on whom punishments of detention have been imposed': Ibid s 3(1).

(j) severe reprimand;

(k) restriction of privileges for a period not exceeding 14 days;

(m) stoppage of leave for a period not exceeding 21 days;

(n) extra duties for a period not exceeding 7 days;

(na) extra drill for no more than 2 sessions of 30 minutes each per day for a period not exceeding 3 days; and

(p) reprimand.[168]

5.120 Some of these penalties, such as imprisonment and fines, are typically characterised as criminal penalties. Dismissal and reprimands are analogous to administrative penalties available under other legislative schemes. The significant difference is that under the DFD Act these types of administrative penalties are available only *after* a conviction.[169]

5.121 The DFD Act sets out restrictions on the power to impose punishments.[170] For example, a service tribunal cannot impose a term of imprisonment on a member of the ADF for an offence against the Act unless it also dismisses the member from the force.[171]

5.122 The *Defence Force Discipline (Consequences of Punishment) Rules 1986* (Cth) set out the consequences of a service tribunal imposing certain of the above punishments on a member of the ADF. For example, restriction of privileges entails, among other consequences, that the member is precluded from: leaving the unit, establishment or ship in which the punishment is to be served except in the course of duty; being present at any recreation or entertainment; and consuming alcohol.[172]

5.123 Offences against s 16 of the DFD Act must be tried before a military judge and military jury.[173] Offences against s 58 can be tried by a military judge sitting alone or with a military jury.[174] Where a s 58 offence is tried by a judge alone, that judge does

168 Some punishments imposed by a summary authority—including detention and reduction in rank—do not take effect unless approved by a reviewing authority under the Act: Ibid s 172.

169 Where a person is convicted by a summary authority, he or she is not required to disclose to any person for any purpose (other than a service one) that the person was convicted of the offence: Ibid s 131B.

170 Ibid s 71.

171 Ibid s 71(1).

172 *Defence Force Discipline (Consequences of Punishment) Rules 1986* (Cth), r 6.

173 Section 16 offences are class 1 offences, and are prescribed for the purpose of s 104(b), which means that a summary authority does not have jurisdiction to try them: see *Defence Force Discipline Act 1982* (Cth) ss 104; 106–7; 108(2), (3); 132A, sch 7; *Defence Force Discipline Regulations 1985* (Cth) reg 44.

174 This is because s 58 offences are Class 3 offences: see *Defence Force Discipline Act 1982* (Cth) s 132AB, sch 7.

not have the power to imprison or detain the offender for a period exceeding six months.[175]

5.124 Offences against s 58 also may be tried by a superior summary authority or a commanding officer if the accused is not a member of the ADF.[176] Where the accused is a member of the ADF, a superior summary authority or commanding officer may have jurisdiction to try an offence against s 58, depending on their ranks relative to the accused.[177]

5.125 There is a significant difference in the punishment that a person who has breached s 58 may receive, depending on: (a) which entity tries the charge; and (b) the rank or status of the person being charged—for example, whether he or she is an officer or member of the ADF.[178] So, if an officer at a specified level is tried for a breach of s 58 by a superior summary authority, the only penalties available are a fine not exceeding the officer's pay for seven days, severe reprimand or reprimand.[179] In contrast, the Australian Military Court may impose: imprisonment; dismissal; reduction in rank; forfeiture of seniority or service for the purpose of promotion; a fine not exceeding the officer's pay for 28 days; a severe reprimand; or a reprimand.[180]

5.126 A superior summary authority or commanding officer must terminate a trial and refer a charge to the Director of Military Prosecutions, if of the opinion that there is sufficient evidence to support a charge, and that the penalties that they have the power to impose under the Act are insufficient to deal with the criminality of the accused's conduct.[181]

Penalties under Cadet Force Regulations

5.127 A member of the cadet force[182] is prohibited under the relevant Code of Conduct from making unauthorised use of confidential information, or revealing it to persons not authorised to receive it.[183]

5.128 Where a member of the cadet force breaches the Code of Conduct, a service chief may impose one or more of the following penalties: formal counselling; reprimand; official warning; reduction in rank; reassignment of duties; suspension of duties; and discharge or termination.[184]

---

175 Ibid sch 2.
176 Ibid ss 106, 107.
177 Ibid ss 106, 107.
178 Ibid schs 2, 3.
179 See Ibid sch 3 cl 1.
180 Ibid sch 2.
181 See Ibid s 131A.
182 Cadet force means the Australian Navy Cadets, the Australian Army Cadets or the Australian Air Force Cadets: *Cadet Force Regulations 1977* (Cth) reg 2.
183 Ibid sch 4(5).
184 Ibid reg 17.

Penalties under Australian Federal Police Act

5.129 The administrative action which may follow breach of a secrecy provision by an appointee of the AFP[185] depends on the category of seriousness of the offence. AFP conduct issues fall into four categories of escalating seriousness:[186]

- category 1: inappropriate conduct that relates to minor management or custom service matters, or reveals a need for improvement in performance, and does not warrant being treated as category 2 or 3 conduct;[187]

- category 2: minor misconduct or inappropriate conduct that reveals unsatisfactory behaviour which would otherwise be category 1 conduct but warrants, because of its repeated nature, to be treated as category 2 conduct;[188]

- category 3: serious misconduct, conduct that raises the question whether termination action should be taken; or conduct that involves a breach of the criminal law or serious neglect of duty, apart from conduct that raises a corruption issue;[189] and

- conduct giving rise to a corruption issue.[190]

5.130 The *Australian Federal Police Categories of Conduct Determination 2006* (Cth) describes conduct that falls within categories 1, 2, and 3. 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'.[191] A more egregious 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.[192]

5.131 Where a manager is satisfied, on reasonable grounds, that an AFP appointee has engaged in category 2 conduct, the manager may take remedial or training and development action, or both against the appointee.[193]

---

185 An AFP appointee is defined to include: a Deputy Commissioner; AFP employee; a special member or special protective service officer: see *Australian Federal Police Act 1979* (Cth) s 4.
186 Ibid s 40RK.
187 Ibid s 40RN.
188 Ibid s 40RO.
189 Ibid s 40RP.
190 Ch 6 discusses the handling and investigation of AFP conduct issues.
191 *Australian Federal Police Categories of Conduct Determination 2006* (Cth), sch.
192 Ibid, sch.
193 *Australian Federal Police Act 1979* (Cth) s 40TJ.

5.132 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.[194]

5.133 Training and development action may take one or more of the following forms:

- coaching or mentoring the AFP appointee;
- making arrangements for the appointee to undertake training or development activities; or
- increasing the level of supervision over the appointee's work.[195]

5.134 Remedial action is defined as action to 'remedy unsatisfactory performance' by an AFP appointee and includes: counselling; issuing a reprimand or a formal warning; requiring the appointee to adopt particular improvement strategies; restricting or reassigning the appointee's duties; or transferring the appointee to another part of the AFP.[196]

5.135 A breach of a secrecy provision will also amount to a breach of the AFP Code of Conduct. The Code requires an AFP appointee to comply with all applicable Australian laws.[197] Breaches of the Code can fall into category 1, 2, or 3 conduct, depending on the gravity of the breach,[198] and therefore will attract the administrative actions relevant to the categorisation of the conduct.

Appropriateness of administrative penalties

5.136 Where a Commonwealth officer breaches a secrecy provision, he or she may be subject to administrative and criminal penalties. The ALRC is interested in eliciting views about whether there are any breaches of secrecy provisions that should only give rise to administrative penalties. A consideration of this issue is informed by the discussion above about when it is appropriate for the criminal law to apply. For example, should the type of penalty imposed depend on: whether the conduct was negligent or reckless as compared to intentional; the type of information protected; or whether harm to the public interest is an element?

Gap in application

5.137 Administrative penalties only apply to current Commonwealth officers. They do not apply to former Commonwealth officers or persons in the private sector who may

194 Ibid s 40TR.
195 Ibid s 40TC.
196 Ibid s 40TD.
197 Australian Federal Police, *AFP Code of Conduct* <www.afp.gov.au> at 31 October 2008.
198 See *Australian Federal Police Categories of Conduct Determination 2006* (Cth), sch.

have access to Commonwealth information. For example, a person who retires from the APS or resigns when an investigation commences is no longer subject to the administrative penalties under the *Public Service Act*. Former Commonwealth officers, however, remain liable under the general secrecy provision in s 70 of the *Crimes Act*.

5.138 Where administrative penalties are unavailable to address breaches of secrecy provisions, in the vast majority of cases the conduct is punishable only by the imposition of criminal penalties.[199] The ALRC is interested in hearing whether it is necessary or desirable to address this gap in application and, if so, by what mechanism or mechanisms.[200]

Consistency of application

5.139 Under the *Public Service Act*, it is within the discretion of each agency head to decide whether to impose an administrative penalty for a breach of the Code of Conduct, and what type of administrative penalty to impose. This creates the potential for disparity among agencies in the application of administrative penalties.

5.140 The House of Representatives Standing Committee on Legal and Constitutional Affairs has noted that:

> The culture of each organisation is a significant variable in any discussion concerning consistency in the application of administrative sanctions. Increased emphasis may be placed on the security of third party information in some departments than others because of the nature of a department's operation. For example, as officers of some departments are subject to legislation which imposes criminal sanctions on the disclosure of particular information, it may be expected that stronger disciplinary action would be taken against those officers than officers in other departments where penal sanctions do not exist.[201]

5.141 The ALRC is interested in hearing whether administrative penalties for breach of similar types of secrecy provisions are being applied consistently across those agencies that are under the umbrella of the *Public Service Act*. The ALRC is also interested in hearing whether administrative penalties for breach of similar types of secrecy provisions are being applied consistently across those Australian Government agencies that do not fall within the ambit of the *Public Service Act*.

---

199 As noted below, to date, the ALRC has identified one civil penalty secrecy provision.

200 The issue of whether there should be a greater role for civil penalties is addressed below.

201 Parliament of Australia—House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995), 81.

Question 5–12 Are the range and level of administrative penalties available for breaches of secrecy provisions committed by Commonwealth officers—for example, the current maximum deduction of 2% of an Australian Public Service employee's annual salary—adequate and appropriate?

Question 5–13 Are there any breaches of secrecy provisions which should only give rise to administrative penalties?

Question 5–14 In circumstances where administrative penalties are unavailable to address breaches of secrecy provisions—namely where such breaches are committed by private sector employees or former Commonwealth officers—are there other ways of addressing this gap in application?

Question 5–15 In practice, are administrative penalties for breach of similar types of secrecy provisions applied consistently across Australian Government agencies? If not, how can this inconsistency best be addressed?

Infringement notices

5.142 An infringement notice is a notice authorised by statute setting out the particulars of an alleged offence. It gives the person to whom the notice is issued the option of either paying the penalty set out in the notice to expiate the offence or electing to have the matter dealt with by a court. Infringement notice schemes typically set penalties at 20% or less of the maximum fine that could be imposed by a court.

5.143 Infringement notices are not administrative penalties in themselves. Rather, they are an administrative device to dispose of a matter involving a breach that would otherwise have to be dealt with by a court—either by way of a criminal prosecution or in civil penalty proceedings.

5.144 To date, the ALRC has not identified any infringement notice schemes in Commonwealth secrecy provisions.[202] However, there is one piece of federal legislation that contains a model infringement notice scheme which, if adopted, would apply to state and territory secrecy provisions. The *National Transport Commission (Model Legislation—Transport of Dangerous Goods by Road or Rail) Regulations 2007* (Cth) set out model legislation intended to be adopted by the states and territories to form part of uniform or nationally consistent legislation relating to road, rail and

202 There are examples of infringement notices schemes in other areas of Commonwealth law. For example, infringement notices are alternative to civil penalty proceedings for alleged breach of continuous disclosure obligations: see *Corporations Act 2001* (Cth) pt 9.4AA. See also *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 497; *Migration Regulations 1994* (Cth) pt 5, div 5.5.

intermodal transport.[203] The model legislation does not itself have the force of law.[204] Regulation 131 is described as a confidentiality provision and it prohibits the unauthorised disclosure of information obtained in the administration of the relevant legislation. Schedule 1.1 sets out recommended penalties, intended to be replaced when the model law is adopted by a state or territory. The recommended penalty for a breach of the confidentiality provision in reg 131 is $2,000 pursuant to an infringement notice or a maximum court-imposed fine of $10,000.[205]

5.145 In *Principled Regulation: Federal Civil and Administrative Penalties in Australia,* the ALRC recommended:

- that in criminal penalty schemes, an infringement notice scheme should apply only to minor offences of strict or absolute liability;

- that in civil penalty schemes, an infringement notice scheme should only apply to minor contraventions in which no proof of a fault element or state or mind is required; and

- a model scheme for infringement notices in Commonwealth regulatory law, features of which included that: the payment of an amount under a notice should not be taken for any purpose to be an admission of liability, and that guidelines should be developed and published by regulators on how they will exercise their discretion to issue, withdraw and correct such notices.[206]

5.146 The ALRC is interested in hearing views about whether infringement notice schemes might have any role to play in offering alternative processes and penalties for enforcing and punishing breaches of Commonwealth secrecy offences.

---

203 *National Transport Commission (Model Legislation—Transport of Dangerous Goods by Road or Rail) Regulations 2007* (Cth) reg 4, schs 1, 2.

204 Ibid reg 4(1).

205 Ibid sch 1.1. The Dangerous Goods Amendment (Transport) Bill 2008 (Vic) has been introduced to facilitate the implementation into the *Dangerous Goods Act 1985* (Vic) of the Commonwealth model law. That bill does not include an infringement notice penalty for breach of a secrecy provision.

206 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Recs 12–1,12–2, 12–8. See also Recs 12–3 to 12–7. Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 51 also expresses the view that an infringement notice scheme should apply only to offences which do not require proof of fault and contain physical elements readily capable of assessment by an enforcement officer.

Question 5–16 Do infringement notice schemes have any role to play in offering alternative processes and penalties for enforcing and punishing breach of Commonwealth secrecy offences? If so, what features should such schemes have?

Civil penalties

5.147 Civil penalties can be characterised as occupying a middle ground between criminal and administrative penalties. 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 contraventions that are not punishable on conviction pursuant to a criminal trial, but are nonetheless actioned by the state in civil proceedings seeking civil penalties.[207] Contraventions of civil penalty provisions are not offences and a declaration that a person has contravened such a provision does not constitute a criminal conviction.

5.148 Most civil penalties are monetary.[208] The appropriate maximum financial penalty under a civil penalty provision can be higher than the maximum fine for a parallel criminal offence. This is justifiable because the adverse effects of a criminal conviction should be taken into account when considering the relative severity of criminal and civil financial penalties.[209]

5.149 In its review of secrecy provisions to date, the ALRC has identified only one civil penalty provision, the breach of which attracts a penalty of $2,200 for a natural person, and $11,000 for a body corporate.[210] The ALRC is interested in hearing views about whether there should be a greater role for civil penalties to apply for unauthorised handling of Commonwealth information and, if so, what model should be adopted. The ALRC is particularly interested in views about the types of secrecy provisions that may more appropriately attract civil, rather than criminal, penalties.

---

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

208 The state may also seek compensation orders consequent on the breach of a civil penalty provision: for example, *Corporations Act 2001* (Cth) ss 1317H, 1317HA.

209 See Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002), Rec 26–3; Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 66.

210 *Workplace Relations Act 1996* (Cth) sch 1, s 276 (unauthorised disclosure of information acquired in inspection of financial records), 306. Breach of this provision is not an offence. *Commonwealth Authorities and Companies Act 1997* (Cth) s 25, although not categorised by the ALRC as a secrecy provision, is an example of another civil penalty provision. It applies to officers or employees of Commonwealth authorities that improperly use information to: gain an advantage for themselves or another person; or cause detriment to a Commonwealth authority or to another person.

5.150 The procedures and rules of evidence in civil cases apply to the enforcement of civil penalty provisions. In criminal proceedings the prosecution must prove its case beyond reasonable doubt.[211] The standard of proof in civil proceedings is on the balance of probabilities[212]—although for serious matters the court may require proof to the higher *Briginshaw* standard of 'reasonable satisfaction'.[213] A regulator's choice of whether to pursue criminal or civil penalties may be determined on the pragmatic ground that the lower evidentiary standard of proof in civil proceedings may increase its prospects of success.

5.151 The interim *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* states that:

> It is particularly important that civil penalties be used in appropriate and justifiable contexts. They are otherwise open to criticism for being too soft (in not carrying a criminal penalty) or for being too harsh (in not carrying the safeguards of criminal procedure such as a requirement for proof beyond reasonable doubt).[214]

5.152 Taking into account recommendations made by the ALRC in its report on civil and administrative penalties,[215] the interim *Guide* 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;
- 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.[216]

5.153 Some Commonwealth legislation adopts a model whereby criminal liability and liability for a civil penalty attach to the same conduct.[217] Often, the distinction between

---

211 *Evidence Act 1995* (Cth) s 141.
212 Ibid s 140.
213 *Briginshaw v Briginshaw* (1938) 60 CLR 336.
214 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 63.
215 Australian Law Reform Commission, *Principled Regulation: Federal Civil & Administrative Penalties in Australia*, ALRC 95 (2002).
216 Australian Government Attorney-General's Department, *Guide to Framing Commonwealth Offences, Civil Penalties and Enforcement Powers* Interim Edition (2007), 63–64.
217 For example, *Corporations Act 2001* (Cth) ss 674, 675; *Environment Protection and Biodiversity Conservation Act 1999* (Cth) ss 20(1)(a), 20A(1).

the two types of liability is that proof of fault, as determined by the application of the *Criminal Code*, is necessary only for criminal liability.[218] Most federal legislation that contains parallel criminal liability and liability for civil penalties:

- allows criminal proceedings to be taken after civil penalty proceedings, regardless of the outcome of the civil case;[219]
- bars civil penalty proceedings after conviction for an offence constituted by conduct that is substantially the same;[220]
- provides for the staying of civil penalty proceedings where criminal proceedings have commenced in respect of conduct that is substantially the same as the conduct alleged to constitute the civil penalty contravention;[221] and
- provides that evidence given in civil penalty proceedings is not admissible in criminal proceedings.[222]

5.154 Other Commonwealth legislation creates separate schemes of liability for civil penalties and criminal liability.[223] Where legislation creates a clear distinction between conduct that attracts criminal liability and conduct that attracts civil penalty liability, most of the problems associated with parallel criminal and civil penalty liability—including use of evidence in more than one proceeding—do not arise.

Question 5–17 Is there a greater role for civil penalties to apply for unauthorised handling of Commonwealth information? If so, what model should apply?

218 There are, however, some civil penalty provisions which contain an element of fault.

219 For example, *Corporations Act 2001* (Cth) s 1317P; *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 486C; *Commonwealth Authorities and Companies Act 1997* (Cth) sch 2, cl 11.

220 For example, *Corporations Act 2001* (Cth) s 1317M; *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 486A; *Commonwealth Authorities and Companies Act 1997* (Cth) sch 2, cl 9.

221 For example, *Corporations Act 2001* (Cth) s 1317N; *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s 486B; *Commonwealth Authorities and Companies Act 1997* (Cth) sch 2, cl 10.

222 For example, *Corporations Act 2001* (Cth) s 1317Q; *Environment Protection and Biodiversity Conservation Act 1999* (Cth) s486D; *Commonwealth Authorities and Companies Act 1997* (Cth) sch 2, cl 12.

223 For example, contraventions of the restrictive trade provisions in *Trade Practices Act 1974* (Cth) pt IV attract civil penalties, while breach of the consumer protection provisions in pt VC attract criminal penalties.

6. Practical Framework for Protecting Commonwealth Information

Contents

Introduction

6.1 The Terms of Reference for this Inquiry ask the ALRC to consider 'relevant … practices relating to the protection of Commonwealth information'.[1] This involves a significantly broader landscape than secrecy provisions in and of themselves, and includes a range of practical, educational and technological strategies aimed at information protection. This chapter discusses the strategies used by the Australian

1 The Terms of Reference are set out at the start of this Issues Paper.

Government to protect Commonwealth information, and asks what improvements could be made in this regard. In particular, it addresses the manner in which breaches are handled and investigated, and the role of bodies tasked to oversee and monitor the information-protection strategies of Australian Government agencies.

Strategies for protecting Commonwealth information

6.2 Secrecy laws do not operate in a vacuum. Australian Government agencies employ a range of strategies to protect Commonwealth information, including by:

- developing and following written policies, manuals and guidelines governing the handling of Commonwealth information, such as the Australian Government Protective Security Manual (PSM), agency policies on information handling, and memorandums of understanding (MOUs);
- raising individual officers' awareness of information-handling obligations through leadership and development programs and oaths of secrecy; and
- implementing infrastructure suitable for handling and securing particular types of Commonwealth information; in particular, information and communication technology (ICT) systems.

6.3 Where an Australian Government agency is aware that unauthorised information handling is about to occur, it also may be able to take preventative action in the civil courts—namely, by seeking an injunction to restrain a possible breach of the criminal law.

6.4 Each of these aspects of the information-handling environment is discussed below.

Australian Government Protective Security Manual

6.5 The PSM is produced and periodically revised by the Protective Security Coordination Centre in the Attorney-General's Department. 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.[2]

6.6 Part C of the PSM deals with information security. The Part

> provides agencies with guidance on the development of security policies that address the issues of awareness, responsibility, behaviour and deterrence to ensure official information is not compromised.[3]

---

2 Protective Security Coordination Centre, *Protective Security Manual (PSM)* (2006) Australian Government Attorney-General's Department, <www.ag.gov.au> at 15 October 2008.

3 Ibid.

6.7 The ALRC considered Part C of the PSM in detail in the 2004 report *Keeping Secrets: The Protection of Classified and Security Sensitive Information* (ALRC 98). The ALRC noted that Part C sets out the following information security principles:

- The availability of information should be limited to those who need to use or access the information to do their work (the 'need-to-know' principle).
- Where the compromise of information could cause harm to the nation, the public interest, the government or other entities or individuals, agencies must consider giving the information a security classification.
- Once information has been identified as requiring security classification, a protective marking must be assigned to the information.
- Once information has been security classified, agencies must observe the minimum procedural requirements for its use, storage, transmission and disposal.[4]

6.8 The PSM distinguishes between national security information and non-national security information.[5] '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 protective 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.[6]

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

---

4 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.

5 The classification system in the PSM is discussed in detail in Ibid, Ch 2.

6 Ibid, [2.9].

- **X-in-Confidence**—if compromise of it could cause 'limited damage' to the Commonwealth, the Government, commercial entities or members of the public;
- **Protected**—if compromise of it could cause 'damage' to the Commonwealth, the Government, commercial entities or members of the public;
- **Highly Protected**—if compromise of it could cause 'serious damage' to the Commonwealth, the Government, commercial entities or members of the public.[7]

6.10 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. Security clearances for non-national security information—Clearances for a Position of Trust—are conducted by individual Australian Government agencies. However, Designated Security Assessment Positions—which allow access to national security information—require an assessment from the Australian Security Intelligence Organisation (ASIO).[8]

6.11 The Australian Government's stated policy is to keep security classified information to the necessary minimum.[9] 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.[10]

6.12 In ALRC 98, the ALRC made a number of recommendations with regard to the PSM and the classification of Commonwealth information. These included, for example, that the PSM should provide more explicit guidance on the classification levels,[11] and include express statements that information should only be classified where there is a clear and justifiable need to do so.[12] The ALRC further recommended that the PSM (with any sensitive protective security information removed) should be placed in the public domain[13]—as is the case in most comparable jurisdictions, such as the United States, the United Kingdom, Canada and New Zealand.[14]

---

7 Ibid, [2.12].
8 Security clearances are discussed in Ibid, Ch 6.
9 Ibid, [2.10].
10 Australian National Audit Office, *Operation of the Classification System for Protecting Sensitive Information*, Audit Report 7 (1999), [2.84].
11 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 4–3.
12 Ibid, Rec 4–5.
13 Ibid, Rec 4–1. At the time of ALRC 98, the PSM did not have a security classification but was not publicly available.
14 Ibid, [4.17].

6.13 The PSM has been revised since the publication of ALRC 98. Unfortunately, however, the document was subsequently given a security classification. The security classification scheme in the revised PSM is broadly consistent with the regime discussed above.[15]

Agency policies and guidelines

6.14 The *APS Values and Code of Conduct in Practice*, issued by the Australian Public Service Commission (APSC), 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.[16]

6.15 Agency policies can play a positive role in protecting Commonwealth information by clarifying and standardising information-handling processes.[17] The relationship between these policies and secrecy laws raises issues. The interaction came into focus, for example, in hearings before the Senate Select Committee on a Certain Maritime Incident (the Children Overboard Affair). The Committee heard evidence about the Department of Defence's public affairs policy, which essentially required all information to be released only by the Minister's media adviser. In its final report on the incident, the Senate Select Committee noted that

> the strictly centralised control of information through the Minister's office … meant that Defence was unable to put out even factual information without transgressing the public affairs plan.[18]

---

15 Australian Government Attorney-General's Department, *Australian Government Protective Security Manual* (2005).

16 Australian Public Service Commission, *APS Values and Code of Conduct in Practice* (2005) <www.apsc.gov.au> at 23 September 2008, ch 3.

17 See, eg, comments about the need to clarify information sharing between the Australian Federal Police and the Australian Security Intelligence Organisation in Australian Federal Police National Security Operations Review Committee, *The Street Review: A Review of Interoperability Between the AFP and its National Security Partners* (2008), [4.2].

18 Parliament of Australia—Senate Select Committee on a Certain Maritime Incident, *Majority Report* (2002), [2.53].

6.16 More recently, following the leak of Cabinet submissions critical of Government policy, the Department of Prime Minister and Cabinet issued an order to its officers to cease providing written coordination comments on Cabinet submissions. Officers were instructed to provide only verbal comments, to minimise the potential for future leaks.[19] However, the Department has now advised that it expects to recommence providing written comments shortly, following the implementation of additional security measures.[20]

6.17 As information-handling policies are not usually publicly available, the ALRC is interested in stakeholder views on the consistency of these policies with secrecy laws—for example, whether agency policies are imposing more restrictive information-handling practices than the related secrecy provisions require.[21]

6.18 An issue also arises in regard to the legal status of agency policies on information handling. Under s 13(5) of the *Public Service Act 1999* (Cth), an Australian Public Service (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'.[22] If an agency's information-handling policy amounts to such a 'lawful and reasonable direction' then an employee who fails to comply with the policy could be the subject of disciplinary proceedings. This could raise particular difficulties where there is inconsistency between the information-handling practices in an agency's policy and requirements under the related secrecy provisions.[23]

Memorandums of understanding

6.19 An MOU does not provide a legal basis for the handling of Commonwealth information. Its operation is dependent upon the conduct—for example, disclosure of information—being authorised by common law or statute. However, entry into an MOU may promote appropriate information sharing among Australian Government agencies. 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'.[24]

6.20 Several Australian Government agencies have MOUs in place relevant to information handling. For example, the Australian Securities and Investments Commission has entered into an MOU with the Australian Government Financial Reporting Council, under which the entities agree (subject to any restrictions imposed

---

19 D Alexander, 'PM Under Fire for 'Paranoia'', *Canberra Times* (Canberra), 21 October 2008, 6.

20 Commonwealth, *Parliamentary Debates*, Senate—Standing Committee on Finance and Public Administration, 20 October 2008, 52 (M Fifield).

21 See Question 6–1 below.

22 *Public Service Act 1999* (Cth) s 13(5).

23 Processes for breach of secrecy obligations are discussed below.

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

by law) to 'share information that they believe would be of assistance to the other in understanding their respective responsibilities under the law'.[25] Each agency agrees, on request, to provide information to the other in a timely manner.[26] 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.[27] Commonwealth and state and territory police departments also have entered into a detailed MOU for the sharing of law enforcement information.[28]

Training and development

6.21 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.[29] In its *State of the Service Report 2001–02*, the APSC reported that agencies alerted employees to their obligations in relation to the non-disclosure of Commonwealth information through:

- the induction process (85% of agencies);
- promulgated policies (58% of agencies);
- Chief Executive instructions (46% of agencies); and
- training programs (44% of agencies).[30]

6.22 The APSC noted, however, that although the majority of employees are informed of their obligations about Commonwealth information when they commence employment, 42% of agencies did not provide employees with regular reminders of these obligations.[31]

6.23 The focus of the APSC's inquiry on training and development programs was the obligation of Commonwealth officers not to disclose information: the ALRC is also interested in hearing whether programs deal with the appropriateness of sharing

---

25 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> cl 4.1.

26 Ibid cl 4.2.

27 Ibid cl 4.3.

28 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*.

29 As discussed in Ch 5, training and development can also be used as an administrative action to address breaches of secrecy laws.

30 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.

31 Ibid, 28–29.

information in particular circumstances.[32] This could apply, for example, where the receiving party 'needs to know' the information in order to carry out his or her functions.

Oaths, affirmations and acknowledgements of secrecy

6.24 A number of secrecy provisions—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.[33] 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.[34] 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.[35]

6.25 Many oaths or affirmations require officers to maintain secrecy 'in accordance with' the associated secrecy provision (or words to this effect). Identical conduct is therefore proscribed in both the oath of secrecy and the head secrecy provision, including the same defences and exceptions. For example, the oath and declaration of secrecy set out in the *Income Tax Regulations 1936* (Cth) requires an officer to swear or declare that he or she

> will not, either directly or indirectly, *except as permitted under the said section*, and either while I am, or after I cease to be, an officer, make a record or divulge or communicate to any person any information respecting the affairs of another person, disclosed or obtained under the provisions of the *Income Tax Assessment Act 1936*, or of any amendment thereof, or of any Act substituted therefore, or of any previous law of the Commonwealth relating to Income Tax.[36]

6.26 It is arguable that the fact that an officer has taken an oath of secrecy has little, if any, legal consequences.[37] Despite their uncertain legal significance, however, oaths

---

32 The Terms of Reference direct the ALRC to have regard to 'the increased need to share such information within and between governments and with the private sector'.

33 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; *Superannuation Guarantee (Administration) Act 1992* (Cth) s 45(8); *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); *Taxation Administration Act 1953* (Cth) s 3C(6); *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.

34 For a discussion of official secrecy provisions that govern Executive Councillors, see P Finn, *Official Information*, Integrity in Government Project: Interim Report 1 (1991).

35 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.

36 *Income Tax Regulations 1936* (Cth) sch 1 (emphasis added).

37 See E Campbell, 'Oaths and Affirmations of Public Office' (1999) 25(1) *Monash University Law Review* 132, 150.

and affirmations may carry with them an imprint of moral significance. As one commentator has noted:

> There is a particular import, a gravitas, to … an oath: a message inherent therein that mandates a sense of trust, be it in oneself to fulfill the promise made or, if we are observing the oath or benefiting from its guarantee, in the oath-taker to do the same.[38]

6.27 The ALRC is interested in hearing views on the role that oaths and affirmations of secrecy play in protecting Commonwealth information.[39]

Information and communication technology systems

6.28 The capacity for Commonwealth officers to handle information appropriately may depend upon the availability of suitable infrastructure—in particular, information and communication technology (ICT) systems. Commonwealth officers have identified improving 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.[40]

6.29 ICT systems have the potential to standardise information-handling practices that may otherwise be contentious or dependent on the favourable exercise of individual discretion. By way of illustration, CrimTrac's National Criminal Investigation DNA Database (NCIDD) provides police with access 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.[41] However, where adequate ICT systems are not available the protection of Commonwealth information can be compromised.[42]

Restrain possible breaches of the criminal law

6.30 In some situations, the Australian Government may be aware that unauthorised handling of Commonwealth information is about to occur. For example, information may have been leaked and publication by the media or on a website appears imminent. In this scenario the Government may have mechanisms available to it to restrain publication.

---

38 N Farid, 'Oath and Affirmation in the Court: Thoughts on the Power of a Sworn Promise' (2006) 40 *New England Law Review* 555, 556. See also J McGinness, 'Secrecy Provisions in Commonwealth Legislation' (1990) 19 *Federal Law Review* 49, 74, which argues that oaths of secrecy reinforce an 'atmosphere of unnecessary secrecy'.

39 See Question 6–2 below.

40 Australian Public Service Commission, *State of the Service Report 2006–07* (2007), 241.

41 CrimTrac, *Annual Report 2006–07* (2007), 18–21.

42 See, eg, comments in PricewaterhouseCoopers, *Australian Taxation Office—Information Security Practices Review Version 2.0* (2008) Australian Taxation Office.

6.31 In ALRC 98, the ALRC analysed potential mechanisms to prevent disclosure of classified and security sensitive Commonwealth information.[43] The ALRC considered that injunctions to restrain a breach of the criminal law provided a potentially appropriate vehicle. However, in the absence of an express statutory power, courts traditionally have been reticent about issuing such injunctions.[44] 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'.[45] 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.[46]

6.32 Section 17B of the *Taxation Administration Act 1953* (Cth), for example, provides that:

> 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.[47]

6.33 In ALRC 98, the ALRC noted the potentially compelling public interest in protecting from disclosure classified and security sensitive information. 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.[48]

6.34 The ALRC is interested in hearing views about whether the same rationale extends to providing courts with express statutory power to grant an injunction to

---

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

44 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.

45 Ibid, 481.

46 *Commonwealth v Fairfax* (1980) 147 CLR 39, 50. Mason J held that s 79 of the *Crimes Act* was not such a provision.

47 *Taxation Administration Act 1953* (Cth) s 17B(1).

48 Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 5–1.

restrain unauthorised handling (or further unauthorised handling) of Commonwealth information other than classified or security sensitive information.

Question 6–1 Are agency policies on information handling consistent with Commonwealth secrecy laws? For example, do agency policies on information handling require a higher level of secrecy than is needed to meet obligations under Commonwealth secrecy laws?

Question 6–2 What role do oaths or declarations of secrecy play in protecting Commonwealth information? Should they be retained?

Question 6–3 How effective are strategies used by Australian Government agencies such as:

(a) memorandums of understanding;

(b) training and development programs; and

(c) information and communication technology systems,

in protecting Commonwealth information? Are there any other strategies for protecting Commonwealth information that the ALRC should consider?

Question 6–4 Should secrecy laws expressly provide for injunctions to restrain unauthorised handling of Commonwealth information? If so, should this apply only to certain types of Commonwealth information, for example, national security or other sensitive Commonwealth information?

Disciplinary processes

6.35 The most common way for Commonwealth agencies to investigate breaches and enforce compliance with secrecy obligations by employees is through administrative proceedings.[49] The manner in which such proceedings are conducted will depend on the conditions under which the employee is employed; in particular, whether the employee is engaged under the *Public Service Act* or under another statutory regime.

6.36 Administrative proceedings will only be applicable to situations where the suspected breach is by an agency employee. Otherwise, enforcement options will be

49 The limited number of criminal prosecutions for breach of a secrecy provision is discussed in Ch 2. In comparison, disciplinary proceedings in regard to unauthorised disclosure of information in Australian Government agencies are more common: see [6.40].

limited to instigating proceedings under criminal law or, where relevant, actions for breach of contract.[50]

Disciplinary action under the *Public Service Act*

APS Code of Conduct

6.37 The *Public Service Act* provides the legal framework for employment in, and management of, the APS. Section 13 of the *Public Service Act* sets out the APS Code of Conduct, which binds APS employees, agency heads and statutory office holders.[51]

6.38 As discussed in Chapter 2, the Code of Conduct sets out how an APS employee should perform his or her functions. Most relevantly, the Code requires 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.[52]

6.39 A finding that an APS employee has breached the Code of Conduct is a necessary precondition for the imposition of administrative penalties.[53]

6.40 In 2006–07, 25 APS employees were investigated in relation to the unauthorised disclosure of information—which was 127% higher than the equivalent number of investigations in 2004–05. A breach of the Code was established in 64% of these investigations.[54]

Identification of suspected breaches

6.41 Investigation of an APS employee for a suspected breach of the Code of Conduct is most commonly triggered through an agency's compliance or monitoring system.[55] A large number of investigations also originate out of conduct identified by supervisors and managers, and conduct identified by work colleagues.[56]

---

50 Criminal proceedings are discussed below. In some limited circumstances civil proceedings may also be instigated: see Ch 5.

51 See *Public Service Act 1999* (Cth) s 14: 'Statutory office holder means a person who holds any office or appointment under an Act, being an office or appointment that is prescribed by the regulations for the purposes of this definition'.

52 *Public Service Regulations 1999* (Cth) reg 2.1(3). Section 13(13) of the *Public Service Act 1999* (Cth) provides that an APS employee must comply with any other conduct requirement prescribed by the regulations.

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

54 Australian Public Service Commission, *State of the Service Report 2006–07* (2007), 126, Table 6.7.

55 Ibid, 120. In 2006–07, these systems accounted for 39% of all Code investigations.

56 Ibid, 120. These accounted for 23% and 21% of Code investigations, respectively. The remainder of investigations were comprised of those initiated by stakeholders or members of the public (10%), and those arising from other sources (4%).

6.42 The APSC has noted the need for agencies to be proactive in providing mechanisms for reporting suspected misconduct, such as through central conduct or ethics units or employee advice or counselling units.[57]

6.43 The *Public Service Act* requires agency heads to establish procedures for protecting APS employees that report breaches, or alleged breaches, of the Code of Conduct to relevant authorities.[58] In 2006–07, only 2% of misconduct investigations stemmed from reports made under an agency's whistleblowing legislation.[59]

Determination of a breach

6.44 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.[60]

6.45 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;[61]
- the process for determining whether an APS employee has breached the Code of Conduct to be carried out informally and expeditiously;[62]
- 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;[63] and
- a written record to be prepared noting the outcome of the investigation.[64]

---

57 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), 23.

58 *Public Service Act 1999* (Cth) s 16.

59 Australian Public Service Commission, *State of the Service Report 2006–07* (2007), 121. Public interest disclosure (whistleblowing) legislation as an exception or defence to secrecy laws is discussed in Ch 4.

60 *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.

61 *Public Service Commissioner's Directions 1999* (Cth) cl 5.2.

62 Ibid cl 5.3.

63 Ibid cl 5.4.

64 Ibid cl 5.5.

6.46 The Australian Government Solicitor (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.[65]

Other processes for handling suspected breaches

6.47 Not all suspected breaches of the Code of Conduct must be dealt with by way of determination.[66] Therefore, a threshold issue for agencies will be whether or not to use the misconduct procedures. The APSC has advised that:

> As a general rule, agencies should use the misconduct procedures if it is likely that they would impose a sanction (either termination of employment, reduction in classification, re-assignment of duties, reduction in salary, a fine or reprimand), if the suspected misconduct was determined to be a breach of the Code.[67]

6.48 Where a decision is made that it is not appropriate to handle the suspected misconduct through agency procedures, alternative options include, for example, dealing with the conduct through the agency's performance management system or the provision of appropriate counselling. An agency also could consider assigning the employee to alternative duties—provided this is not perceived as a de facto penalty.[68]

6.49 The procedural fairness obligations discussed above do not apply where an agency deals with misconduct in a way other than through disciplinary proceedings.[69]

Penalties

6.50 The *Public Service Act* sets out an exhaustive list of the penalties that an agency head can impose on an employee who has been found to have breached the Code of Conduct.[70] However, the APSC has advised that—provided it is clearly cast as management action and not a penalty—other action may be warranted in order to reduce the risk of further misconduct.[71] In the context of unauthorised disclosure of information, this hypothetically could involve restricting an employee's access to certain information.

---

65 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

66 *Public Service Commissioner's Directions 1999* (Cth) cl 5.1 note.

67 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), 30.

68 Ibid, 31.

69 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

70 *Public Service Act 1999* (Cth) s 15(1). Administrative penalties under the *Public Service Act* are discussed in detail in Ch 5.

71 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.

Suspension of employment and reassignment of duties

6.51 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.[72]

6.52 Suspension is subject to the following conditions:

- Other than in exceptional circumstances, suspension without remuneration is to be for no longer than 30 days.[73]
- The agency head must review the suspension at reasonable intervals.[74]
- The agency head must immediately end the suspension if he or she no longer believes on reasonable grounds that the APS employee has, or may have, breached the Code of Conduct; or that suspension is in the public, or agency's, interest.[75]
- 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.[76]

6.53 An agency head is normally required to exercise his or her powers of suspension having 'due regard for procedural fairness'.[77] This requirement need not apply where the agency head is satisfied, on reasonable grounds, that it would not be appropriate in the circumstances.[78] However, it would be unusual for a decision maker to be satisfied on a reasonable basis that according procedural fairness would not be appropriate. 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.[79]

6.54 An agency head also determines whether a suspension is to be with or without remuneration. Factors that may influence this decision include, for example, the

---

72 *Public Service Regulations 1999* (Cth) reg 3.10.
73 Ibid reg 3.10(3).
74 Ibid reg 3.10(4).
75 Ibid reg 3.10(5).
76 Ibid reg 3.10(6).
77 Ibid reg 3.10(7).
78 Ibid reg 3.10(7).
79 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

seriousness of the suspected misconduct and the estimated duration of the misconduct proceedings.[80]

6.55 As an alternative to suspension, an agency head may temporarily reassign an employee's duties while the employee is investigated for a suspected breach of the Code of Conduct.[81] Other than in limited situations, an employee is not entitled to a review of a reassignment of duties.[82]

Review of findings of breach

6.56 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).[83] Where a person's employment has been terminated, the employee may seek redress under the *Workplace Relations Act 1996* (Cth). Employees also have the right to seek judicial review by the Federal Court of the agency-level decision under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (ADJR Act) or pursuant to s 39B of the *Judiciary Act 1903* (Cth).

6.57 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?[84]

6.58 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

---

80 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.

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

82 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), 33. A reassignment may be reviewed where it involves a reduction in classification, relocation to another place, or duties that the employee cannot reasonably be expected to perform. Ibid, 33.

83 *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*: ibid reg 5.23(2).

84 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.

substitute a new action for the action that was under review.[85] 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.[86] In 2007–08, the MPC reported that 'virtually all recommendations made in relation to applications for review of action were accepted in full by the relevant agency heads'.[87]

Agency heads

6.59 Agency heads are expressly bound by the Code of Conduct. The *Public Service Act* does not, however, specify the penalties that may be imposed on an agency head who breaches the Code of Conduct. The APS Commissioner is given power to inquire into alleged breaches of the Code of Conduct by agency heads and to report to the appropriate authority (usually the Prime Minister or other relevant minister) on the results of such enquiries, including recommendations for penalties where appropriate.[88]

Question 6–5 In practice, how effective are the processes set out in the *Public Service Act 1999* (Cth) and related instruments for investigating and enforcing suspected breaches of secrecy provisions that amount to breaches of the Code of Conduct?

Other disciplinary procedures

6.60 The disciplinary provisions discussed above apply only to 'APS employees'. A large number of persons potentially subject to administrative penalties for breach of Commonwealth secrecy laws are employed other than under the *Public Service Act*.[89] Disciplinary provisions that attach to these persons vary on:

- whether or not the provisions are located in the employing agency's or authority's enabling legislation;
- whether, where the enabling Act is silent on a particular issue, the provisions of the *Public Service Act* apply; and
- the availability of merits review of disciplinary decisions.

---

85 *Public Service Regulations 1999* (Cth) reg 5.32.
86 *Public Service Act 1999* (Cth) s 33(6).
87 Australian Public Service Commissioner, *Annual Report 2007–08* (2008), 101.
88 *Public Service Act 1999* (Cth) s 41(1)(f).
89 For example, the definition of 'Commonwealth officers'—whose conduct is regulated by s 70 of the *Crimes Act*—expressly includes persons employed: in the Australian Defence Force; in the service of a Commonwealth public authority; in the AFP; and by the Australian Postal Corporation: *Crimes Act 1914* (Cth) s 3.

6.61 Disciplinary processes relevant to the principal categories of Commonwealth officers employed otherwise than under the *Public Service Act* are addressed below. These include those applicable to: employees of the AFP; employees of ASIS and ASIO; members of the Australian Defence Force (ADF); and employees of statutory authorities.

Australian Federal Police

6.62 The procedures for raising and dealing with misconduct in the AFP are established by Part V of the *Australian Federal Police Act 1979* (Cth) (AFP Act).[90]

6.63 Both the manner in which an 'AFP conduct issue'[91] is dealt with under the regime and the penalties that may be imposed depend on the category of seriousness of the conduct issue:

- Category 1, being the lowest and least serious;
- Category 2, being the next highest and next most serious;
- Category 3, being the next highest and next most serious; and
- conduct giving rise to a corruption issue, which is the highest and most serious.[92]

6.64 The *Australian Federal Police Categories of Conduct Determination 2006* (Cth) prescribes what behaviour falls within each of these categories. Breach of a secrecy provision could constitute either a Category 2 or a Category 3 conduct issue, depending on its egregiousness.[93]

6.65 Category 1 and 2 conduct issues are dealt with managerially. The AFP Act sets out detailed procedural requirements for the manner in which these issues must be handled.[94] These include requirements for a manager to:

- ensure that the AFP officer and the complainant (if any) have an adequate opportunity to be heard in relation to the issue;

---

90 The regime was introduced in the *Law Enforcement (AFP Professional Standards and Related Measures) Act 2006* (Cth).

91 'AFP conduct issues' are defined in s 40RH of the *Australian Federal Police Act 1979* (Cth).

92 Ibid s 40RK.

93 Category 2 conduct issues include 'Information misuse (access or inadvertent disclosure)', including, for example, accidental or unintentional access or disclosure of information. Category 3 conduct issues include: 'Information Misuse', such as 'improperly disclosing or failing to protect from improper disclosure, sensitive information held by the AFP'; and 'Information Access', which includes 'unlawfully or improperly accessing AFP information'. *Australian Federal Police Categories of Conduct Determination 2006* (Cth).

94 *Australian Federal Police Act 1979* (Cth) pt V div 3 subdiv C.

- ensure that the AFP officer is involved, as far as practicable, in the resolution of the issue; and

- determine what action (if any) is to be taken in relation to the issue.[95]

6.66 More formal investigation processes apply to Category 3 conduct issues and corruption issues. Investigations are conducted by an allocated officer of an AFP unit specifically constituted to undertake investigations of misconduct engaged in by AFP appointees.[96] The Commonwealth Ombudsman must be notified of any investigation of a Category 3 conduct issue.[97]

6.67 Investigators are provided with broad investigative powers.[98] Provided the relevant laws are complied with,[99] the investigation generally may be conducted in such manner as the investigator thinks fit.[100] The investigator is empowered to direct an AFP officer to give information, or produce a document, and failure to comply with such an order is an offence.[101]

6.68 On completion, the investigator must provide a written report of the results of the investigation.[102] The AFP Commissioner is responsible for ensuring that any recommendations made in the report are 'fully considered' and that 'appropriate action' is taken in relation to the issue.[103] There is no requirement however for the Commissioner's action to correlate with the action recommended by the investigator.[104]

6.69 The AFP Act formally links misconduct investigations and consideration of 'AFP practices issues'—that is:

> an issue of whether a practice or procedure of the Australian Federal Police is or has been:
>
> (a) contrary to law; or

---

95 Ibid s 40TH. An equivalent obligation is placed on an investigator of a Category 3 conduct issue or corruption issue: *Australian Federal Police Act 1979* (Cth) s 40TQ.

96 *Australian Federal Police Act 1979* (Cth) s 40RD. Where the issue relates to a member of the section, or it would otherwise be inappropriate for the issue to be investigated by a member of the unit, the Commissioner must allocate the issue to a suitably qualified person who is not a member of the unit: ibid s 40TO.

97 Ibid s 40TM(1).

98 These powers are additional to any other powers that the investigator may have: Ibid s 40VA.

99 Ibid s 40VD.

100 Ibid s 40VB(2).

101 Ibid s 40VE(3). However, the information obtained in accordance with such a direction is only admissible in evidence against the AFP officer in any civil or criminal proceedings in limited circumstances.

102 Ibid s 40TU.

103 Ibid s 40TV.

104 Ibid s 40TR(2).

(b) unreasonable, unjust, oppressive or improperly discriminatory; or

(c) inadequate; or

(d) otherwise wrong or inappropriate.[105]

6.70 Where an investigator of a misconduct issue is satisfied that the information raises an AFP practices issue, the investigator must bring the practices issue to the attention of an appropriate AFP appointee (for Category 1 and 2 conduct issues)[106] or include the issue and appropriate recommendations in his or her report (for Category 3 and corruption issues).

6.71 Decisions made in relation to AFP conduct issues can be appealed to the Federal Court of Australia for judicial review under the ADJR Act or s 39B of the *Judiciary Act*.[107] As with APS employees, an action to terminate the employment of an AFP appointee can be appealed to the Australian Industrial Relations Commission.[108] However, there is no provision for the Administrative Appeals Tribunal, or an alternative merits review body, to review decisions under the Act.

ASIO and ASIS

6.72 Unlike other officers of the Australian Intelligence Community (AIC), employees of ASIO and the Australian Secret Intelligence Service (ASIS) are not employed under the *Public Service Act*.

6.73 Under s 86 of the *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act), the terms and conditions of employment of officers and employees of ASIO 'shall be such as are determined from time to time by the Director-General'. The Act provides only minimal requirements for such employment conditions—principally, that an officer's employment can only be terminated in accordance with a term or condition of his or her employment.[109] Information on the terms and conditions of ASIO employment is not publicly available; however, ASIO advises that 'ASIO's conditions of service are similar to those of the Australian Public Service'.[110]

6.74 The legislative basis for the work of ASIS is the *Intelligence Services Act 2001* (Cth). As with ASIO, the Director-General of ASIS may determine the terms and

---

105 Ibid s 40RI(2). 'Practices and procedures' is defined at *Australian Federal Police Act 1979* (Cth) s 40RI(3).

106 *Australian Federal Police Act 1979* (Cth) ss 40TK, 40TW.

107 An exception to the right of judicial review applies to decisions made under s 40TF of the AFP Act to take no further action in relation to AFP conduct or practices issue: *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 10.

108 *Australian Federal Police Act 1979* (Cth) s 69B, which retains the operation of pt 12, div 4 of the *Workplace Relations Act 1996* (Cth).

109 *Australian Security Intelligence Organisation Act 1979* (Cth) s 89. The Act also provides that the regulations may deal with matters relating to employment conditions for temporary and casual staff; ibid s 90. No such regulations have been made.

110 Australian Security and Intelligence Organisation, *Conditions of Service* (2008) <www.asio.gov.au/Careers/Content/Conditions.aspx> at 10 October 2008.

conditions on which employees are to be employed. However, the Director-General of ASIS is obliged to consult with affected employees about these conditions.[111] 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.[112]

6.75 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.[113] The procedures must include:

> (a) initial consideration of grievances by the Director-General or a person authorised in writing by the Director-General;
>
> (b) establishment of Grievance Review Panels chaired by independent Chairs to make determinations reviewing initial consideration of grievances.[114]

Members of the Australian Defence Force

6.76 The *Defence Force Discipline Act 1982* (Cth) (DFD Act) establishes the disciplinary regime applicable to ADF members suspected of committing a 'service offence',[115] two of which involve secrecy: 'Communicating with the enemy' (s 16 offences);[116] and 'Unauthorised disclosure of information' (s 58 offences).[117]

6.77 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, when required; conduct investigations; and provide evidence to support prosecutions of service offences.[118] The provisions for investigation of service offences 'follow an altered version of the requirements ordinarily applied to civilian criminal investigation'.[119] Where an ADF member is

---

111 *Intelligence Services Act 2001* (Cth) s 33.

112 Ibid s 355.

113 Ibid s 37.

114 Ibid s 37(3). The Director-General also must implement a determination of a Grievance Review Panel to the extent that it is within his or her power to do so. *Intelligence Services Act 2001* (Cth) s 37(4).

115 The ADF also has in place an administrative system. Adverse administrative action may be taken in relation to conduct that does not constitute criminal conduct or warrant the initiation of disciplinary proceedings under the DFD Act: Parliament of Australia—Senate Foreign Affairs Defence and Trade References Committee, *The Effectiveness of Australia's Military Justice System* (2005), 18.

116 *Defence Force Discipline Act 1982* (Cth) s 16.

117 Ibid s 58.

118 Parliament of Australia—Senate Foreign Affairs Defence and Trade References Committee, *The Effectiveness of Australia's Military Justice System* (2005), [3.8].

119 *White v Director of Military Prosecutions* [2007] HCA 29, [98]. See: *Defence Force Discipline Act 1982* (Cth) pt VI, div 6.

charged with a service offence, or is reasonably suspected of having committed a service offence, an authorised officer may suspend the member from duty.[120]

6.78 The manner in which a charge for breach of a service offence is dealt with—and the potential punishment for any finding of breach[121]—depends on the 'service tribunal' to which it is appointed: a summary authority; or the Australian Military Court (AMC).[122] This allocation depends on:

- **Jurisdictional issues:** The AMC has jurisdiction to try any charge against any person.[123] In contrast, the jurisdiction of a summary authority depends on the respective rank of the authority and the ADF member who is the subject of the charge.[124] Certain service offences cannot be tried by summary authorities, including offences punishable by more than two years imprisonment.[125] Consequently, a s 16 offence must always be heard by the AMC.[126]

- **Discretion:** A commanding officer (CO) has discretion to determine the manner in which a service offence charge is handled, including by: trying the charge himself or herself; directing that it not be proceeded with; referring it to another summary authority; or referring it to the Director of Military Prosecutions (DMP), an independent prosecutorial authority.[127] Where a charge is referred to the DMP (either through the CO or otherwise),[128] the DMP may request that it be referred to the AMC.[129]

- **Request by the accused person:** Prior to a charge being dealt with by a summary authority, the accused person is entitled to elect to have the charge tried by the AMC.[130]

6.79 Summary authorities comprise officers of the ADF, appointed from within the chain of command. Summary authorities try service offences in a manner broadly akin to a civilian criminal trial, involving an initial plea of guilty or not guilty; a hearing to determine whether there is sufficient evidence to support the charge; the giving of testimony and other evidence where the trial continues; and sentencing.[131] Detailed

120 *Defence Force Discipline Act 1982* (Cth) s 98.
121 Penalties for secrecy offences under the *Defence Force Discipline Act* are discussed in Ch 5.
122 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.
123 Ibid s 115. there is an exception, however, for 'custodial offences'.
124 Ibid ss106–108.
125 *Defence Force Discipline Regulations 1985 (Cth)* reg 44.
126 Section 16 of the *Defence Force Discipline Act* carries a maximum penalty of 15 years imprisonment.
127 *Defence Force Discipline Act 1982* (Cth) s 110.
128 A charge may also be referred to the DMP: directly through the Provost Marshall; or by a summary authority which has been allocated the charge: Ibid ss 109, 111.
129 Ibid s 103. The DMP also may direct that the charge not be proceeded with, or refer the charge to a summary authority: *Defence Force Discipline Act 1982* (Cth) s 103.
130 *Defence Force Discipline Act 1982* (Cth) s 111B.
131 Ibid s 130.

procedural requirements are included in the *Summary Authority Rules 2008* (Cth), reflecting many due process requirements at general law.[132] However, there also are 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.[133]

6.80 The AMC is a permanent military court independent of the ADF chain of command. The AMC is comprised of military judges, who are serving members of the ADF appointed by the Minister.[134] Depending on its seriousness, an offence may be dealt with by a military judge alone or by military judge and military jury.[135] Proceedings in the AMC are conducted in accordance with the *Australian Military Court Rules 2007* (Cth).[136]

6.81 An ADF member who has been convicted by a summary authority can appeal to the AMC against his or her conviction, or a punishment imposed.[137] An automatic review process also applies to all proceedings heard by a summary authority.[138] Decisions of the AMC can be appealed to the Defence Force Discipline Appeal Tribunal;[139] and, from the Tribunal, questions of law can be appealed to the Federal Court.[140] However, decisions under the DFD Act are expressly excluded from judicial review under the ADJR Act.[141] Further, as members of the ADF are not 'employees' at common law they do not fall within the scope of the unfair dismissal regime in the *Workplace Relations Act*.[142]

---

132 The Rules include, eg, a right to silence for the accused person: *Summary Authority Rules 2008* (Cth) r 41; and a requirement to give reasons for a finding of guilt, and any punishment or order imposed: ibid r 38.

133 Ibid r 12(3). An accused person being tried by the AMC must be afforded advice and representation by a legal officer. *Defence Force Discipline Act 1982* (Cth) s 137.

134 Military judges also must have been enrolled as a legal practitioner for a minimum of five years. *Defence Force Discipline Act 1982* (Cth) s 188AR.

135 For those offences classified 'class 1' military offences, it is mandatory for trial to be by military judge and military jury: Ibid s 132A. This includes s 16 offences: *Defence Force Discipline Act 1982* (Cth) sch 7. Part 6 of the *Australian Military Court Rules 2007* (Cth) provide for an accused person to elect the mode of trial.

136 The Rules, for example, oblige the Chief of the ADF to secure witnesses 'reasonably required by the accused person'; allow for the questioning of witnesses; and set out jury selection procedures.

137 *Defence Force Discipline Act 1982* (Cth) s 161.

138 Ibid ss 151–152. If the reviewing authority considers the conviction to be unreasonable, wrong in law or fact, or otherwise unsafe or unsatisfactory, the authority must recommend to the ADF member that he or she consider appealing to the AMC: *Defence Force Discipline Act 1982* (Cth) s 155.

139 The Defence Force Discipline Appeal Tribunal is established under the *Defence Force Discipline Appeals Act 1955* (Cth).

140 Ibid s 52.

141 *Administrative Decisions (Judicial Review) Act 1977* (Cth) sch 1(o). Those constituting the service tribunals are 'officers of the Commonwealth' for the purpose of s 75(v) of the *Australian Constitution*; therefore, an action for judicial review may be brought under s 39B of the *Judiciary Act*.

142 See *Williams v Commonwealth of Australia* [2000] AIRC 428.

6.82 The disciplinary regime in the DFD Act has been subject to significant legal and political controversy. First, questions have been raised about the framework's constitutionality—that is, whether trials for service offences require an exercise of the judicial power of the Commonwealth within the meaning of Ch III of the *Australian Constitution*.[143] More broadly, in 2005, the Senate Standing Committee on Foreign Affairs, Defence and Trade noted recurring deficiencies in the operation of the system, including the investigation process and the operation of service tribunals.[144] Accordingly, the committee recommended that all 'non-military' offences should be referred to civilian authorities for investigation and prosecution.[145]

Statutory authorities

6.83 There are over 160 statutory authorities in the Commonwealth sphere,[146] characterised by diverse legal frameworks and governance structures. For many of these authorities, the statutory office holder and his or her staff constitute a 'statutory agency' within the meaning of the *Public Service Act*. In such cases, the administrative framework in the *Public Service Act* applies—including the APS Code of Conduct and procedures for suspected breach of the Code.

6.84 For statutory authorities other than those that fall within the *Public Service Act*, the terms and conditions under which staff members are to be employed are usually left to a Certified Agreement or the discretion of the authority itself, or a particular person or persons within the authority. The *Australian Postal Corporation Act 1989* (Cth) further 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.[147]

6.85 The terms and conditions of appointment of statutory office holders generally are at the discretion of the responsible minister or the Governor-General.

---

143 The AMC is not a court established under Ch III of the Australian Constitution: *Defence Force Discipline Act 1982* (Cth) s 114. This issue was considered in *White v Director of Military Prosecutions* [2007] HCA 29. The High Court upheld the service tribunal framework. In dissent, Kirby J held that service tribunals were only constitutional for 'disciplinary offences', rather than offences of a 'substantially criminal character'.

144 Parliament of Australia—Senate Foreign Affairs Defence and Trade References Committee, *The Effectiveness of Australia's Military Justice System* (2005).

145 Ibid, recs 1–3. The Australian Government rejected these recommendations; however, it has implemented other significant reforms to the military justice system including, for example, the AMC.

146 Statutory authorities are public sector entities created by legislation. J Uhrig, *Review of the Corporate Governance of Statutory Authorities and Office Holders* (2003), 16.

147 *Australian Postal Corporation Act 1989* (Cth) s 90. This Act also sets out terms and conditions for the termination of a director's employment by the Governor-General: see s 79. See also *Australian Broadcasting Corporation Act 1983* (Cth) ss 32, 33; *Special Broadcasting Service Act 1991* (Cth) ss 54, 55.

Question 6–6 In practice, how effective are the processes for investigating and enforcing breaches of secrecy laws by Commonwealth officers other than Australian Public Service (APS) employees? In particular, should the legislation under which these officers are employed:

(a) require that the processes for dealing with suspected misconduct that apply to APS employees be adopted, to the extent that these processes are consistent with the performance of the functions of the employing agency; and

(b) include a process for merits review of any penalties imposed?

Criminal investigations

6.86 In most situations, the Australian Government will only become aware of an unauthorised handling of Commonwealth information after the breach has occurred. Whether criminal proceedings are instigated in relation to the breach will depend on decisions at several critical crossroads in the prosecutorial pathway—the first being the decision to commence an investigation.

6.87 The decision whether to initiate investigative action ordinarily rests with the agency responsible for administering the relevant legislation.[148] Actual investigation of the possible or alleged criminal conduct, however, is usually carried out by the AFP.

6.88 Where an agency reports to the AFP a suspected breach of a secrecy law, the AFP decides whether to accept or reject the matter for investigation on the basis of the *Case Categorisation and Prioritisation Model* (CCPM). The CCPM is intended to provide

> a transparent, objective and consistent basis for evaluating and comparing AFP operational activities from a range of perspectives, including across agencies, regions (geographic locations) or teams (work groups).[149]

6.89 The AFP completes a CCPM rating at the time an incident is referred, taking into account such issues as the:

- incident and case type;

148 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <www.cdpp.gov.au/Publications/ProsecutionPolicy/> at 26 August 2008, [3.2].

149 Australian Federal Police, *Case Categorisation and Prioritisation Model* (2006), 1.

- impact of the matter on Australian society;
- importance of the matter to the referring agency and the AFP; and
- resources required by the AFP to undertake the matter.[150]

6.90 Alternatively, an agency may instigate an independent investigation of a potential breach of a secrecy provision. This could be undertaken, for example, for minor or routine incidents that are unlikely to be accepted by the AFP under the CCPM. Where an agency obtains sufficient evidence it may subsequently refer the matter to the Commonwealth Director of Public Prosecutions (CDPP) for consideration of prosecution.

6.91 An issue that arises is whether there is sufficient transparency in decisions by agencies or the AFP to initiate investigations into suspected breaches of secrecy laws, particularly in light of the political nature of some breaches of secrecy laws. In the context of an AFP raid on the home of fellow *Canberra Times* reporter, Philip Dorling, to determine the source of a leak of classified information, Jack Waterford commented that:

> Police diligence in making an investigation [of a leak] has always seemed very closely related to whether government, of any persuasion, has actually wanted a result—a point Sir Humphrey Appleby made clear in many episodes of *Yes Minister*. Police, pretending to be independent, play the game from the moment they get the call—a reason why decisions about raids are always 'informed', even if police insist that they are not 'involved'.[151]

Question 6–7 Is there sufficient transparency in decisions to investigate breaches of secrecy provisions, for example through the *Case Categorisation and Prioritisation Model*?

Prosecutorial discretions and processes

Commencing prosecutions

6.92 The CDPP is an independent prosecuting agency established under the *Director of Public Prosecutions Act 1983* (Cth). Decisions by the CDPP to initiate criminal proceedings are made in accordance with the *Prosecution Policy of the*

150 Ibid, 3.

151 J Waterford, 'A Very Leaky Case', *The Canberra Times* (Canberra), 27 September 2008, 1. In comparison, see Commonwealth, *Parliamentary Debates*, Senate, 10 September 2003, 14835 (J Faulkner—Leader of the Opposition in the Senate), where the then Government was accused of failing to investigate the release of confidential information for political purposes.

Commonwealth.[152] This document expressly states that the prosecution of suspected criminal offences should not be automatic. Rather, the decision to prosecute should be made only where an offence, or the circumstances of its commission, is of such a nature that a prosecution is required in the public interest.[153] Factors relevant to the public interest include, for example:

- the seriousness or triviality of the alleged offence;
- the degree of culpability of the alleged offender;
- the availability and efficacy of any alternatives to prosecution;
- the prevalence of the alleged offence and the need for deterrence; and
- the likely length and expense of a trial.[154]

6.93 The *Prosecution Policy of the Commonwealth* also outlines a number of factors which 'must clearly not' influence a decision whether or not to prosecute, being:

> (a) the race, religion, sex, national origin or political associations, activities or beliefs of the alleged offender or any other person involved;
>
> (b) personal feelings concerning the alleged offender or the victim;
>
> (c) possible political advantage or disadvantage to the Government or any political group or party; or
>
> (d) the possible effect of the decision on the personal or professional circumstances of those responsible for the prosecution decision.[155]

6.94 As discussed in Chapter 2, offending conduct may satisfy the elements of multiple Commonwealth secrecy laws. The *Prosecution Policy of the Commonwealth* provides guidance on the decision about what charge or charges should be laid where the evidence discloses an offence against several different laws. That is, where the available evidence will support charges under both a provision of a specific Act and one or more of the offences of general application in the *Crimes Act*, the provisions of the specific Act ordinarily should be used. In some situations, however, reliance on the specific provisions may not 'adequately reflect the nature of the criminal conduct

---

152 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <www.cdpp.gov.au/Publications/ProsecutionPolicy/> at 26 August 2008.
153 Ibid.
154 Ibid, [2.10].
155 Ibid, [2.13].

disclosed by the evidence'.[156] This discretion may be exercised, for example, where penalties for *Crimes Act* offences are higher than the penalties under a specific Act.[157]

6.95 The prosecution also plays a major role in the decision about whether to proceed summarily or on indictment. Factors relevant to determining whether or not a case is appropriate for trial on indictment include: the nature and seriousness of the offence; the adequacy of sentencing options if the case were determined summarily; and the greater publicity, and therefore the greater deterrent effect, of a conviction obtained on indictment.[158]

Attorney-General's consent to prosecution

6.96 The consent of the Attorney-General must be obtained before a prosecution can be initiated for a breach of some secrecy provisions. For example, the Attorney-General, or a person acting under his or her direction, must consent for a prosecution for a breach of the secrecy provisions set out in ss 79 (official secrets) and 83 (unlawful soundings) of the *Crimes Act* to be instigated.[159] Other secrecy provisions where the consent of the Attorney-General is required for commencing prosecutions include:

- s 91.1 of the *Criminal Code* (Cth), dealing with espionage and similar activities;[160]
- ss 18 and 92 of the *Australian Security Intelligence Organisation Act 1979* (Cth), which govern communication of intelligence by officers of ASIO, and publication by any person of the identity of an officer of ASIO, respectively;
- various provisions of the *Intelligence Services Act 2001* (Cth), including the communication of information prepared by or on behalf of ASIS, the Defence Imagery and Geospatial Organisation (DIGO) or the Defence Signals Directorate (DSD) by officers of the respective agency;[161] and the publication by any person of the identity of the staff of these agencies;[162] and
- s 9 of the *Defence (Special Undertakings) Act 1952* (Cth), governing unlawful entry to 'prohibited areas'.[163]

---

156 Ibid, [2.22].
157 Ibid, [2.21].
158 Ibid, [5.9]–[5.10]. See also Australian Law Reform Commission, *Same Crime, Same Time: Sentencing of Federal Offenders* (2006).
159 *Crimes Act 1914* (Cth) s 85. These provisions are set out in full in Appendix 3. Significantly, however, no equivalent requirement for consent applies for prosecutions of breaches of s 70 of the *Crimes Act*.
160 *Criminal Code* (Cth) s 93.1.
161 *Intelligence Services Act 2001* (Cth) ss 39, 39A and 40, respectively.
162 Ibid s 41. See also *Intelligence Services Act 2001* (Cth) sch 1, pt 2, which requires the consent of the Attorney-General to prosecute members of the Committee on Intelligence and Security.
163 *Defence (Special Undertakings) Act 1952* (Cth) s 28.

6.97 Other types of offences that require the Attorney-General's consent in order to commence prosecutions include:

- sedition;[164]
- those involving harming Australians outside of Australian territory;[165] and
- genocide, crimes against humanity, war crimes and crimes against the administration of justice in the International Criminal Court.[166]

6.98 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.[167] The *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'.[168]

6.99 The ALRC's report on sedition laws, *Fighting Words*, noted concerns about the political nature of consent requirements.[169] Specifically, the Attorney-General, as a political figure, might be perceived to agree more readily to the prosecution of certain persons—such as those who criticise government policy or are unpopular with the electorate. Politicisation also may arise where the Attorney-General refuses consent; for example, to prosecute of a person who is perceived to be politically aligned to the government of the day.[170] As a consequence, the ALRC recommended removing the requirement for the Attorney-General's consent to prosecutions of sedition offences.[171]

---

164 *Criminal Code* (Cth) s 80.5.

165 Ibid s 115.6.

166 Ibid s 268.121.

167 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <www.cdpp.gov.au/Publications/ProsecutionPolicy/> at 26 August 2008, [2.25]. The requirement for the Attorney-General to consent to prosecution was held out as a significant safeguard for introducing the secrecy offence provision in the *Crimes Act*. Commonwealth, *Parliamentary Debates*, House of Representatives, 21 October 1914, 264 (W Hughes—Attorney General).

168 Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth* <www.cdpp.gov.au/Publications/ProsecutionPolicy/> at 26 August 2008, [2.27].

169 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006). See Ch 13.

170 Ibid, [13.2]–[13.24]. The ALRC recommended removing the consent requirement in s 80.5 of the *Criminal Code* (Cth): Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Rec 13–1.

171 Australian Law Reform Commission, *Fighting Words: A Review of Sedition Laws in Australia*, ALRC 104 (2006), Rec 13–1.

6.100 The ALRC is interested in hearing views on the appropriateness of requiring the consent of the Attorney-General for prosecutions for breaches of certain secrecy laws.

Question 6–8 Should the Attorney-General's consent be required for the commencement of prosecutions under:

(a) ss 79 or 83 of the *Crimes Act 1914* (Cth) or s 91.1 of the *Criminal Code* (Cth);

(b) secrecy provisions relating to national security and other sensitive Commonwealth information; or

(c) any other secrecy provisions?

Managing overlapping proceedings

Concurrent administrative and criminal proceedings

6.101 A Commonwealth officer suspected of breaching a secrecy law may be subject to both administrative and criminal proceedings.[172] In its Legal Briefing, *Misconduct in the Australian Public Service*, the AGS noted:

> 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.[173]

6.102 The APSC has advised that an agency generally should not proceed with a misconduct action if the police or prosecuting authorities consider that this action could prejudice criminal proceedings.[174] Ultimately, however, the decision whether to proceed with administrative proceedings in parallel with the criminal process is at the discretion of the relevant agency.

---

172 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.

173 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

174 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.

6.103 Concurrent criminal and disciplinary proceedings may give rise to practical difficulties. This has occurred, for example, in the context of an accused's right to silence. An APS employee subject to Code of Conduct proceedings may decline to provide information on the basis of the privilege against self-incrimination.[175] However:

> 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.[176]

6.104 In *Goreng Goreng v Jennaway*,[177] Flick J considered whether an agency's review of an employee's suspension in connection to a Code of Conduct investigation should be postponed. The applicant argued that, as she was choosing to exercise her right of silence in the associated criminal proceedings, she would be unable to fully participate in the administrative hearing. Although 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', he held that this 'does not ordain the postponement, perhaps for an indefinite period, of an administrative process'.[178] In the absence of any legislative provisions to the contrary, Flick J held that whether or not administrative processes are postponed pending the resolution of criminal proceedings was a discretionary matter for the agency.

Question 6–9 Is there a need for any safeguards to apply where secrecy provisions could give rise to both administrative and criminal proceedings; for example, should the legislation provide for a stay of administrative proceedings to accommodate current or future criminal actions?

'Security incidents'

6.105 A suspected breach of a secrecy law also could fall within the ambit of a 'security incident'—being an activity or occurrence that compromises, or has the potential to compromise, official resources (including official information).[179]

---

175 P Vermeesch, *Legal Briefing No 80: Misconduct in the Australian Public Service* (2006) Australian Government Solicitor.

176 Ibid.

177 *Goreng Goreng v Jennaway* [2007] 164 FCR 567.

178 Ibid, [48]–[50].

179 Australian National Audit Office, *Administration of Security Incidents, Including the Conduct of Security Investigations*, Audit Report 41 (2005), [1.6].

6.106 In its audit of the administration of security incidents by Commonwealth agencies, the ANAO noted the differing aims of a security investigation (a formal tool used to assess the implications of a security incident) and other investigations undertaken by agencies, such as those into suspected misconduct:

> The aim of a security investigation is to prevent the incident from re-occurring by making improvements to systems or procedures. It is not necessarily the purpose to establish guilt and aid the prosecution of an offender, as may be the case in a fraud investigation.[180]

6.107 The ANAO recommended that agencies should develop documentation relating to the administration of security incidents and the conduct of security investigations. This should include guidance on distinguishing between the actions required for security investigations, and investigations into matters not related to security.[181]

Overseeing the protection of Commonwealth information

Commonwealth Ombudsman

6.108 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.[182] This potentially includes a range of agency practices for protecting Commonwealth information—for instance, a decision by an agency or officer to disclose, or not disclose, information to a third party. The Ombudsman is expressly prevented, however, from investigating employment action (for example, a penalty for a determined breach of the APS Code of Conduct) taken in respect of APS employees.[183]

6.109 After completing an investigation, the Ombudsman must make a report to the relevant agency or authority, including recommendations for change, where he or she is of the opinion:

> (a) that the action:
>
> (i) appears to have been contrary to law;
>
> (ii) was unreasonable, unjust, oppressive or improperly discriminatory;
>
> (iii) was in accordance with a rule of law, a provision of an enactment or a practice but the rule, provision or practice is or may be unreasonable, unjust, oppressive or improperly discriminatory;
>
> (iv) was based either wholly or partly on a mistake of law or of fact; or
>
> (v) was otherwise, in all the circumstances, wrong;

---

180 Ibid, [2.5].
181 Ibid, rec 1. Each of the entities audited by the ANAO agreed with this recommendation.
182 *Ombudsman Act 1976* (Cth) s 5. The Ombudsman has additional responsibilities in his or her associated role as the Defence Force Ombudsman; Law Enforcement Ombudsman; Immigration Ombudsman; Postal Industry Ombudsman; and Taxation Ombudsman.
183 Ibid s 5(2)(d).

(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.[184]

6.110 The Ombudsman has no power to implement the conclusions of his or her investigation directly. However, if appropriate action is not taken, the Ombudsman can make a further report to the Prime Minister.[185] The Ombudsman also must file annual reports that are tabled in both Houses of Parliament.[186]

Australian Public Service Commissioner

6.111 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 Code of Conduct.[187]

6.112 Under s 44 of the Act, the Commissioner is required to prepare a report to the Prime Minister, for presentation to Parliament, on the state of the APS during the preceding financial year. Every year the APSC sends a questionnaire to each agency seeking information on which to base the report. Agency heads are required to provide the Commissioner with the information needed to prepare the report.[188]

6.113 The *Public Service Act* also establishes the role of the MPC.[189] 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.[190] Recommendations made by the MPC are not legally binding; however, if the MPC is not satisfied with an agency's

184 Ibid s 15(1).
185 Ibid s 16.
186 Ibid s 19.
187 *Public Service Act 1999* (Cth) s 41(1)(a), (b).
188 Ibid s 44(3).
189 Ibid pt 6.
190 Ibid s 33.

response to recommendations, he or she may, after consulting with the responsible Minister, give a report on the matter to the minister of the responsible agency and to either or both of the Prime Minister and the Presiding Officers, for presentation to Parliament.[191] 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.[192]

Australian National Audit Office

6.114 Under the *Auditor-General Act 1997* (Cth), the Auditor-General—supported by the 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, and accountability. This function is primarily fulfilled by conducting performance and financial statement audits.[193] The ANAO has conducted a series of audits of the policies and practices used by Commonwealth agencies to protect their resources, including Commonwealth information.[194]

Overseeing specific sectors

Australian Taxation Office

6.115 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.

---

191 Ibid s 33(5), (6).

192 Ibid s 50.

193 Australian National Audit Office, *About Us* (2006) <www.anao.gov.au/director/aboutus.cfm> at 5 September 2008.

194 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).

6.116 Where the Inspector-General, in the course of his or her review, forms the opinion that a tax official has engaged in misconduct, the Inspector-General must report the evidence to the Commissioner of Taxation.[195]

Australian Federal Police

6.117 The Commonwealth Ombudsman, in his or her role as Law Enforcement Ombudsman, has an enhanced investigatory and inspection role in relation to the AFP. The AFP must notify the Ombudsman of all serious misconduct matters dealt with under the AFP Act.[196] The Ombudsman must undertake an annual review of the administration of AFP conduct and practices issues,[197] a copy of which must be provided to both the President of the Senate and the Speaker of the House of Representatives for tabling.[198] Further, the Ombudsman may, at any time, inspect the records of AFP conduct and practices issues dealt for the purposes of conducting an ad hoc review of the administration of AFP conduct and practices issues.[199]

6.118 The Law Enforcement Integrity Commissioner is responsible for preventing, detecting and investigating serious and systemic corruption issues in the AFP and the Australian Crime Commission.[200] The jurisdiction of the Integrity Commissioner potentially could be invoked, for example, where unauthorised handling of Commonwealth information is associated with financial gain on the part of an officer.

Australian Intelligence Community

6.119 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory office holder who reviews the activities of the agencies which collectively comprise the Australian Intelligence Community (AIC)—the Office of National Assessments (ONA), ASIO, the DSD, the Defence Intelligence Organisation (DIO), the DIGO and ASIS. 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.[201]

---

195 Inspector-General of Taxation Act 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).

196 *Australian Federal Police Act 1979* (Cth) s 40TM.

197 Ibid pt V div 7.

198 Ibid s 40XD.

199 Ibid s 40XB.

200 *Law Enforcement Integrity Commissioner Act 2006* (Cth).

201 Inspector-General of Intelligence and Security, *About IGIS* (2008) <www.igis.gov.au/about.cfm> at 7 October 2008.

6.120 The IGIS considers complaints or requests from ministers in relation to the actions of AIC agencies; investigations also can be initiated by his or her own motion. In undertaking inquiries, the IGIS has investigative powers akin to those of a Royal Commission. Where the IGIS completes an inquiry, he or she must provide a report, including any conclusions and recommendations, to the head of the relevant agency and to the responsible minister.[202] The agency head must advise the IGIS of any action taken in response to the inquiry. Where the IGIS is of the view that such action is inadequate or inappropriate, he or she may discuss the matter with the responsible minister and prepare a report, a copy of which is provided to the Prime Minister.[203]

6.121 Additional oversight of the AIC is provided by the Parliamentary Joint Committee on Intelligence and Security (PJCIS). The PJCIS is required, under s 29(1)(a) of the *Intelligence Services Act*, to conduct an annual review of the administration, expenditure and financial statements of the AIC. The PJCIS does not conduct inquiries into individual complaints about the AIC agencies' activities.

Australian Defence Force

6.122 The Inspector-General of the ADF (IGADF) is a statutory position introduced in 2005 to oversee the ADF military justice system.[204] 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.[205]

6.123 The IGADF does not have the power directly to implement measures arising out of his or her investigations. Rather, the IGADF may report the outcome of inquiries to the Chief of the ADF, an official in the Department of Defence, a member of the ADF or another person affected by the inquiry.[206] The Department of Defence's annual report also includes a section on the operation of the Office of the IGADF.

6.124 Additional oversight of the ADF is provided by the Defence Force Ombudsman (DFO), another office of the Commonwealth Ombudsman. The DFO can investigate administrative actions related to or arising out of a person's service in the ADF, either following receipt of a complaint or on the DFO's own motion.[207] In general, before the DFO will investigate a complaint from an ADF member, the member must first have

---

202 *Inspector-General of Intelligence and Security Act 1986* (Cth) s 22.
203 Ibid s 24.
204 *Defence Act 1903* (Cth) pt VIIIB. The position of the IGADF was introduced in the *Defence Legislation Amendment Act (No. 2) 2005* (Cth).
205 Australian Government Department of Defence, *Annual Report 2006–07* (2007), 156.
206 *Defence (Inquiry) Regulations 1985* (Cth) reg 102(3).
207 *Ombudsman Act 1976* (Cth) s 19C(2), (3).

exhausted internal grievance mechanisms. The DFO is not authorised to investigate disciplinary action taken against an ADF member.[208]

Question 6–10 In practice, how effective are the mechanisms in place for monitoring and overseeing the application and enforcement of secrecy laws by Commonwealth agencies?

Question 6–11 Are there any other issues relating to the practical framework for protecting Commonwealth information that the ALRC should consider?

208 Ibid s 19C(5)(d).

7. Comparisons and Interactions with Other Laws

Contents

Introduction

7.1 The information-handling matrix of any jurisdiction is highly contingent on history and culture. Indigenous groups in Australia, for example, have well-established rules governing disclosure of information, which may be based on a complex range of factors such as group membership, status, age and gender.[1] The United Kingdom (UK) traditionally has had a secretive culture surrounding government information, grounded

1 See, eg, Australian Law Reform Commission, *Recognition of Aboriginal Customary Laws*, ALRC 31 (1986), Ch 25; M Langton, 'The Hindmarsh Island Bridge Affair: How Aboriginal Women's Religion Became an Administrable Affair' (1996) 11 *Australian Feminist Studies* 211.

in the historical role and position of the Crown.[2] On the other hand, in the United States (US), government information is relatively more accessible, in part because this jurisdiction is not informed by the 'Westminster system' of government.[3] Government operations in Sweden are far more transparent than in the US, but a great deal of personal information about individuals is also made available online by government.[4] In contrast, the UK, US and Australia have legislative regimes that, to varying degrees, restrict disclosure of information about individuals.[5]

7.2 Chapter 1 of this Issues Paper provides a brief description of the range of secrecy laws. In Chapter 2, the ALRC provides an historical overview of secrecy laws in Australia. In this Chapter, the ALRC considers the relationship between Commonwealth secrecy laws and other Commonwealth laws that deal with handling of information. The ALRC asks what changes, if any, need be made to these laws to ensure an appropriate balance between the protection of Commonwealth information and an open and accountable system of government—a hallmark of a modern democratic society. The ALRC also considers the intersection between secrecy provisions and the regulation of information privacy.

---

2 The *Official Secrets Act* was first enacted in the UK in 1889. See also E Campbell, 'Public Access to Government Documents' (1976) 41 *Australian Law Journal* 73, 77. Note, however, that the *Freedom of Information Act 2000* (UK) came into force in January 2005.

3 The Westminster system of government also is discussed in Chs 1 and 2. In the US, legislation establishing rights of access to government records in limited circumstances was enacted in 1946, and legislation establishing a general right of access was enacted in 1966: *Administrative Procedure Act of 1946* 60 Stat 237 (US) and *Freedom of Information Act of 1966* 80 Stat 383 (US). See also J Michael, 'Freedom of Information in the United States of America' in N Marsh (ed) *Access to Government-Held Information* (1987) 55. There has also been some discussion about whether the First Amendment to the United States Constitution may give rise to a general right of access to government information: R Jolly, 'The Implied Freedom of Political Communication and Disclosure of Government Information' (2000) 28 *Federal Law Review* 42, 50–51. However, the Bush administration has taken a number of steps to erode access to government information: W Loegering, *The Secret President—Congress Resists a Decline in Executive Transparency* (Fall 2008) Harvard Political Review <http://hprsite.squarespace.com/the-secret-president-112008/> at 11 November 2008. In November 2008, a US media coalition called on President-elect Obama to restore and promote access to government information: Sunshine in Government Initiative—Media Coalition, 'Recommendations for Action by the Obama Administration to Strengthen Transparency and Integrity in Government' (Press Release, 10 November 2008).

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

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

Freedom of information

Overview of the *Freedom of Information Act 1982* (Cth)

7.3 Freedom of information (FOI) laws are aimed at enhancing public access to government records. At the federal level, the main law governing FOI is the *Freedom of Information Act 1982* (Cth) (FOI Act).[6]

7.4 The FOI Act forms part of a package of legislation based on the principle of government openness and accountability. There are several areas of accountability that 'together provide a framework for control of government action'.[7] FOI legislation is a component in the range of administrative law mechanisms, which includes courts, tribunals, oversight bodies—such as the Ombudsman and the Inspector-General of Intelligence and Security—and legislation that confers rights on members of the public to obtain access to government documents and to be provided with reasons for decisions.

7.5 The FOI Act provides a right of access to information held by government agencies and ministers. Access is provided both through an obligation to publish certain information[8] and also a right to apply for the production of documents.[9] The FOI Act also gives a person a right to annotate or correct personal records held by government agencies.[10]

7.6 The long title of the FOI Act emphasises its focus on access: 'An Act to give to members of the public rights of access to official documents of the Government of the Commonwealth and of its agencies'. This is spelled out in s 3 which states that the object of the Act is:

> to extend as far as possible the right of the Australian community to access to information in the possession of the Government of the Commonwealth by:
>
> (a) 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; and

---

6 In 1995, the ALRC and Administrative Review Council made a number of recommendations for reform of FOI laws and practices: Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995). These recommendations are discussed below. In Ch 2 of this Issues Paper, the ALRC provides an historical overview of the introduction of the FOI Act.

7 Ibid.

8 *Freedom of Information Act 1982* (Cth) pt II.

9 Ibid, pt III.

10 Ibid, pt V.

> (b) creating a general right of access to information in documentary form in the possession of Ministers, departments and public authorities, 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; and
>
> (c) creating a right to bring about the amendment of records containing personal information that is incomplete, incorrect, out of date or misleading.[11]

7.7 This focus is further emphasised in s 3(2):

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

7.8 However, the principle of open government, which a right of access enshrines, has to be balanced with the practical need of a government to be able to govern and, for that purpose, to be able to keep some documents protected from disclosure. The public interest in protecting certain information from disclosure is reflected in the exemption provisions, the purpose of which is 'to balance the objective of providing access to government information against legitimate claims for protection'.[12] The fact that there are listed exemptions, therefore, expresses a countervailing public interest to that of disclosure.

7.9 On 24 September 2007, the then Attorney-General, the Hon Philip Ruddock MP, requested that the ALRC inquire into FOI laws and practices across Australia.[13] On 22 July 2008, this inquiry was deferred by the new Australian Government as part of its FOI reform process.[14] The Cabinet Secretary and Special Minister for State, Senator the Hon John Faulkner, has stated that the Australian Government will introduce a Bill to remove the power to issue conclusive certificates in FOI and archives legislation before the end of 2008, and will release an exposure draft bill for further FOI reform early in 2009.[15] Developments in this area will be of relevance to the ALRC in the course of this Inquiry.

---

11 Ibid, s 3(1).

12 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), [8.1].

13 P Ruddock (Attorney-General), 'Australian Law Reform Commission to Examine FOI Laws' (Press Release, 24 September 2007).

14 J Faulkner (Cabinet Secretary and Special Minister for State), 'Freedom of Information Reform' (Press Release, 22 July 2008).

15 J Faulkner (Cabinet Secretary and Special Minister for State), *Transparency and Accountability: Our Agenda, 30 October 2008* (2008) <http://www.smos.gov.au/speeches/2008/sp_20081030.html> at 30 October 2008. Senator Faulkner has stated areas of intended reform: the establishment of a Federal Information Commissioner; removal of fees to access information; and implementation of other recommendations contained in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).

Exemptions for certain agencies and documents

7.10 Section 7 of the FOI Act provides a complete exemption for certain agencies, including the Australian Secret Intelligence Service (ASIS), the Australian Security Intelligence Organisation (ASIO), the Office of National Assessments (ONA) and the Inspector-General of Intelligence and Security (IGIS).

7.11 Other Commonwealth agencies that handle a significant amount of material relating to national security, such as the Department of Foreign Affairs and Trade, the Department of Immigration and Citizenship, and the Australian Federal Police, are open to FOI applications. However, s 7(2A) provides an exemption for all agencies in relation to documents that originate with, or have been received from, ASIS, ASIO, ONA, Defence Intelligence Organisation, Defence Signals Directorate or the IGIS.

7.12 In addition, access to documents may be denied on the basis of one of the specific grounds of exemption under Part IV of the FOI Act. These exemptions include: documents affecting national security, defence or international relations;[16] Cabinet documents;[17] internal working documents;[18] documents relating to business affairs;[19] and documents affecting the national economy.[20]

7.13 For example, s 33(1) provides that:

> A document is an exempt document if disclosure of the document under this Act:
>
> (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.

7.14 If access to a document is denied on the basis that the document falls within an exemption category, a person may nevertheless still be provided with a copy of that document with exempt material deleted, as long as this is reasonably practicable.[21]

---

16 *Freedom of Information Act 1982* (Cth) s 33.
17 Ibid, s 34.
18 Ibid, s 36.
19 Ibid, s 43.
20 Ibid, s 44.
21 Ibid, s 22.

The secrecy exemption

7.15 Secrecy provisions in other enactments can be invoked by a government agency or minister to refuse access to a document under the FOI regime. Section 38 of the FOI Act (the secrecy exemption) provides that documents, or information contained in documents, subject to certain secrecy provisions do not need to be disclosed under the FOI Act. The secrecy exemption may apply to documents or information if a secrecy provision prevents disclosure, and:

- is set out in Schedule 3 of the FOI Act;[22] or
- enlivens the secrecy exemption by expressly applying s 38 of the FOI Act.[23]

7.16 The secrecy exemption applies only to the extent that a secrecy provision prohibits disclosure to the person making the FOI request.[24] 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,[25] and s 503A of the *Migration Act 1953* (Cth) does not apply.[26] Finally, a person cannot be prosecuted under a secrecy provision if that person discloses in good faith a document that is the subject of an FOI request under the FOI Act.[27]

Background

7.17 The secrecy exemption to FOI was intended to preserve the operation of existing Commonwealth secrecy provisions. In 1979, the Senate Standing Committee on Legal and Constitutional Affairs released a report on the Freedom of Information Bill 1978 (Cth) and the Archives Bill 1978 (Cth).[28] The Committee was concerned about the wide ambit of the proposed secrecy exemption, and recommended that it should only apply to prescribed secrecy provisions contained in a schedule to the Bill.[29] Secondly, the Committee was of the view that 'all criminal provisions prohibiting or restricting the disclosure of information that are not prescribed under the Bill should be repealed'.[30]

---

22 Ibid, s 38(1)(b)(i).
23 Ibid, s 38(1)(b)(ii).
24 Ibid, s 38(1A).
25 *Re Richardson and Federal Commissioner of Taxation* (2004) 81 ALD 486, 503; *Petroulias v Commissioner of Taxation* [2006] AATA 333, [65]–[66].
26 *Freedom of Information Act 1982* (Cth), s 38(2), (3). *Migration Act 1958* (Cth) s 503A is discussed below.
27 *Freedom of Information Act 1982* (Cth) s 92(1)(b). See also *Actors' Equity v Australian Broadcasting Tribunal* (1984) 6 ALD 68, 80–81.
28 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).
29 Ibid, Rec 21.13(a).
30 Ibid, Rec 21.13(c).

7.18 The Committee's second recommendation was not taken up, and the first recommendation was not immediately implemented. A broadly worded secrecy exemption was contained in the FOI Act as enacted in 1982.[31] In 1991, however, the FOI Act was amended to include Schedule 3, as well as the requirement that secrecy provisions either be listed in this Schedule, or expressly apply the secrecy exemption.[32]

7.19 Currently, Schedule 3 contains over 50 provisions in 28 Acts and one sub-regulation. This list includes provisions of the *Australian Security Intelligence Organisation Act 1979* (Cth), *Intelligence Services Act 2001* (Cth), *Child Support (Assessment) Act 1989* (Cth) and *Designs Act 2003* (Cth).

7.20 Schedule 3 has been amended several times since its introduction. The provisions in 11 Acts have been removed entirely from the list,[33] provisions in nine new Acts added to the list,[34] and a number of provisions in remaining Acts amended.[35] In addition, since 1991, a number of provisions in other Acts have expressly applied s 38 of the FOI Act with respect to certain information.[36] Some of these provisions are also listed in Schedule 3,[37] others are not.[38]

7.21 What if a secrecy provision is not listed in Schedule 3 and does not expressly apply the secrecy exemption in s 38? This issue arose in the Federal Court decision *Kwok v Minister for Immigration and Multicultural Affairs*.[39] The effect of that decision was that s 503A of the *Migration Act* enlivened the secrecy exemption in the FOI Act even though that provision was not listed in Schedule 3 of the FOI Act, nor did it expressly apply the secrecy exemption.[40] Tamberlin J reached his decision on the basis that s 503A(8) is 'cast in comprehensive language' such as to provide that s 503A

---

31 The original s 38 of the FOI Act provided that: A document is an exempt document if there is in force an enactment applying specifically to information of a kind contained in the document and prohibiting persons referred to in the enactment from disclosing information of that kind, whether the prohibition is absolute or is subject to exceptions or qualifications.

32 *Freedom of Information Amendment Act 1991* (Cth) ss 28, 47.

33 Deletions from the original Schedule 3 include: *Wool Tax (Administration) Act 1964* (Cth) ss 8(2), (5) (repealed) and *Social Security Act 1991* (Cth) ss 1312(1), 1336(2). Provisions in the *Designs Act 1906* (Cth) were replaced by provisions in the *Designs Act 2003* (Cth).

34 Additions of legislative provisions enacted since 1991 include: *Aged Care Act 1997* (Cth) ss 86–2(1), s 86–5–86–7 and *Gene Technology Act 2000* (Cth) ss 187(1), (2).

35 Secrecy provisions added to enactments already listed in the Schedule 3 include: *Telecommunications (Interception) Act 1979* (Cth) s 133 and *Taxation Administration Act 1953* (Cth) ss 3G, 3H and 355−5 in Schedule 1.

36 See, eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(11); *Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992* (Cth); *Reserve Bank Act 1959* (Cth) s 79A(9).

37 See, eg, the notes contained in *Gene Technology Act 2000* (Cth) s 197 and *Migration Act 1958* (Cth) s 503A.

38 See, eg, *Australian Prudential Regulation Authority Act 1998* (Cth) s 56(11).

39 *Kwok v Minister for Immigration and Multicultural Affairs* (2001) 112 FCR 94.

40 *Migration Act 1958* (Cth) s 503A restricts the disclosure by Commonwealth officers of information supplied by law enforcement agencies or intelligence agencies.

overrides a requirement to provide information in another Act that does not expressly exclude its operation.[41]

7.22 In 2003, a new subsection was added to s 38 of the FOI Act 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.[42]

7.23 On 31 December 2007, the Department of Prime Minister and Cabinet released an updated version of the *FOI Guidelines—Exemption Sections in the FOI Act* (the Guidelines). The Guidelines are described as a 'reference tool' and do not replace the operation of exemptions in the Act.[43] The Guidelines note that the secrecy exemption 'should be used only where truly necessary' and that information may be more appropriately considered under other exemptions in the FOI Act. The Guidelines also state that the exemption is not intended to include information that is 'identified by reference only to the manner or capacity in which it is received'.[44]

Previous inquiries and the secrecy exemption

7.24 The secrecy exemption has been considered in a number of previous inquiries. In 1995, the ALRC and the Administrative Review Council (ARC) Report, *Open Government* (ALRC 77),[45] recommended that the secrecy exemption should be repealed,[46] on the basis that the other FOI exemptions, such as those dealing with personal information and national security and defence, provided sufficient protection of government-held information covered by secrecy provisions. The ALRC and ARC also noted the submission by the Department of Social Security that the 1994 amendments to the *Social Security Act 1991* (Cth) that removed the secrecy exemption

---

41 *Kwok v Minister for Immigration and Multicultural Affairs* (2001) 112 FCR 94, 99. This is the case regardless of whether a relevant Act was enacted before or after the commencement of s 503A of the *Migration Act 1958* (Cth). This decision was overturned by the Full Federal Court, but the secrecy exemption was not considered on appeal. See also M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.99].

42 *Migration Legislation Amendment (Protected Information) Act 2003* (Cth) Sch 2.

43 Department of Prime Minister and Cabinet, *FOI Guidelines—Exemption Sections in the FOI Act* (2007) <www.dpmc.gov.au> at 14 October 2008. Agency policies for information handling, which may include FOI matters, are discussed in Ch 6.

44 Ibid, [9.1.4]. See also Australian Government Attorney-General's Department, *Freedom of Information Act 1982—Fundamental Principles and Procedures* (2005) <http://www.pmc.gov.au/> at 21 November 2008.

45 Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995). Earlier inquiries that considered the secrecy exemption include: 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) and H Gibbs, R Watson and A Menzies, *Disclosure of Official Information: Review of Commonwealth Criminal Law* (1988).

46 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.

for FOI applications to the Department had not adversely affected the operations of the Department.[47]

7.25 The ALRC and ARC concluded that:

> the exemption provisions in the FOI Act represent the full extent of information that should not be disclosed to members of the public. Secrecy provisions that prohibit the disclosure of information that would not fall within the exemption provisions are too broad. The Review considers that repealing s 38 will promote a more pro-disclosure culture in agencies.[48]

7.26 The ALRC and ARC also suggested that, if the secrecy exemption were not repealed, it should be amended so that Schedule 3 provides a definitive list of all secrecy provisions that affect the operation of the FOI Act.[49]

7.27 In 2001, several recommendations made in ALRC 77 were considered by the Senate Legal and Constitutional Affairs Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000* (the Senate Committee Inquiry).[50] In its submission to the Senate Committee Inquiry, the Australian Government Attorney-General's Department opposed the repeal of s 38 of the FOI Act.

> In the Department's view, the exemptions in the FOI Act are, of necessity, in general terms whereas the secrecy provisions in other legislation are tailored to the specific requirements of that legislation and may cover situations, not covered by the FOI Act, which nevertheless warrant exemption from disclosure.[51]

7.28 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'.[52]

An appropriate balance between secrecy and open government?

7.29 One issue in this Inquiry is whether the secrecy exemption inappropriately prevents disclosure of information that is the subject of formal FOI requests. Another issue is whether the operation of secrecy provisions contradicts a fundamental premise

---

47 Ibid, [11.3].
48 Ibid, [11.3].
49 Ibid, [11.3].
50 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of information Amendment (Open Government) Bill 2000* (2001). This Bill was introduced by Democrats Senator Andrew Murray in 2000, and would have implemented several of the recommendations made by the ALRC and the ARC in Australian Law Reform Commission and Administrative Review Council, *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).
51 Parliament of Australia—Senate Legal and Constitutional Legislation Committee, *Inquiry into the Freedom of information Amendment (Open Government) Bill 2000* (2001), [3.35].
52 Ibid, [3.34]–[3.36].

of the FOI Act. There is a discrepancy between the objects of the FOI Act—with its presumption of general access to information—and the application of criminal and administrative penalties for informal disclosure in accordance with the intention of the FOI Act.[53]

7.30 A person who follows the spirit of the FOI Act and discloses a document without having received a formal FOI request may commit a breach of a secrecy provision that would not have been breached if the information had been released pursuant to an FOI application. It has been observed that:

> the question is no longer the substance of disclosure, but the process by which it happens … the issue is who makes the decision to release [the records], not whether they are released at all.[54]

7.31 The ALRC is interested in hearing about whether the relationship between secrecy provisions and the FOI Act strikes the right balance between protecting Commonwealth information and preserving open and accountable government in Australia. If there is an imbalance, how should it be addressed? For example, should disclosure in accordance with the objects of the FOI Act override a secrecy provision that does not fall within the current exemptions in the FOI Act, to address the situation outlined above?

7.32 In addition, should ss 7 and 38 of the FOI Act be amended or repealed? Does the *Archives Act 1983* (Cth) model of setting out specific exemptions, discussed further below, provide a better way of determining when access to documents should be restricted?

Question 7–1 Given that the *Freedom of Information Act 1982* (Cth) promotes open and accountable government, and secrecy provisions protect Commonwealth information, what should be the relationship between these two regimes?

Question 7–2 If the relationship between secrecy provisions and the *Freedom of Information Act 1982* (Cth) (FOI Act) does not strike the right balance, how should this be addressed? For example:

---

53 A person who makes an informal disclosure in accordance with the object of the FOI Act does not receive the same protection as a person who makes a formal disclosure under the Act. Moira Paterson has described the 'chilling effect' of secrecy provisions in this context: M Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (2005), [8.106]. Also see the discussion of public interest disclosure (or 'whistleblowing') legislation in Ch 4.

54 C Erskine, 'The Bennett Decision Explained: The Sky is not Falling!' (2005) 46 *Australian Institute of Administrative Law (AIAL) Forum* 15, 18.

(a) should it be clarified that disclosure in accordance with the objects of the FOI Act overrides a secrecy provision that does not fall within the current exemptions in the Act?

(b) should the secrecy exemption in the FOI Act be amended or repealed?

Question 7–3 Are there other aspects of the relationship between secrecy provisions and the *Freedom of Information Act 1982* (Cth) that need to be clarified?

Privacy

Overview of the *Privacy Act 1988* (Cth)

7.33 The *Privacy Act 1988* (Cth) aims to protect personal information about individuals and give them some control over how that information is collected, stored, used and disclosed. It also gives individuals rights of access to, and correction of, their own personal information.[55]

7.34 The *Privacy Act* contains safeguards set out in a number of Information Privacy Principles (IPPs) and National Privacy Principles (NPPs), which have the force of law.[56]

7.35 The IPPs cover 'personal information' which is collected or in a 'record' held by an 'agency', as those terms are defined in the Act. With limited exceptions, these agencies include only Australian Government and ACT public sector entities.[57] The NPPs cover personal information collected or held in a record by certain private sector organisations.[58] 'Organisation' is defined as an individual, a body corporate, a partnership, any other unincorporated association or a trust.[59] The *Privacy Act* applies

55 The ALRC recently conducted a major inquiry into Australian privacy laws: see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008).

56 *Privacy Act 1988* (Cth) s 14 (IPPs), sch 3 (NPPs).

57 'Agency' is defined to include ministers, departments, federal courts and other bodies established for a public purpose: Ibid s 6(1).

58 The *Privacy Amendment (Private Sector) Act 2000* (Cth) came into operation on 21 December 2001 and extended the coverage of the *Privacy Act* to much of the private sector. The private sector provisions of the *Privacy Act* apply to 'organisations', which include partnerships, unincorporated associations and bodies corporate. An individual who is self-employed or a sole trader is considered an organisation for the purposes of the *Privacy Act*. Organisations are generally responsible for the actions of their employees, contractors and subcontractors, all of which are covered by the *Privacy Act:* ss 6C, 8. In Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), the ALRC recommended that there should be a unified set of privacy principles that regulates both agencies and organisations: Rec 18–2.

59 *Privacy Act 1988* (Cth) s 6C.

to 'acts and practices'; that is, acts done and practices engaged in by agencies or organisations.

7.36 'Personal information' is defined as

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.[60]

7.37 Personal information includes written or electronic records about individuals, such as social security records and medical records, but may also include photos or videos, where the person can be identified from the context or in other ways. A person's name appearing on a list of clients may also fall within the definition of personal information because the context provides information, possibly sensitive personal information, about the individual.

7.38 'Sensitive information' is a sub-set of personal information and is given a higher level of protection under the NPPs. 'Sensitive information' is defined as health or genetic information about an individual or personal information or an opinion about an individual, including that individual's racial or ethnic origin, political opinions, religious beliefs or affiliations or sexual preferences or practices.[61]

7.39 The *Privacy Act* contains a range of exemptions and exceptions, which are found throughout the Act, in the definition of some terms, in specific exemption provisions and in the IPPs and NPPs themselves. The acts and practices of some Australian Government agencies—including the intelligence agencies ASIS, ASIO and ONA—are completely exempt from the *Privacy Act.*[62]

7.40 While information that is subject to secrecy provisions is generally handled by a government agency and is therefore subject to the IPPs, some secrecy provisions regulate organisations that 'stand in the shoes' of a Commonwealth officer, or secondary disclosure to other organisations, which may then be covered by the NPPs.

7.41 The Federal Privacy Commissioner has a number of statutory functions in relation to handling complaints, investigating breaches, and enforcing the *Privacy Act*. Under Part V of the Act, the Commissioner has the power to investigate complaints,[63]

---

60 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.

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

62 Ibid, s 7. In ALRC 108, the ALRC expressed the view that the current exemptions that apply to the intelligence and defence intelligence agencies under the *Privacy Act* should remain: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [34.94]–[34.109].

63 *Privacy Act 1988* (Cth), s 40.

obtain information and documents[64] and examine witnesses.[65] The Commissioner's determinations may be enforced by proceedings in the Federal Court of Australia or the Federal Magistrates Court.[66]

7.42 The *Privacy Act* addresses specific secrecy provisions in Part VIA of the Act.[67] This Part makes special provision for the collection, use and disclosure of personal information in emergencies or disasters. Section 80P(1) provides that when an emergency declaration is in force, an entity may collect, use or disclose personal information in certain circumstances. Section 80P(2) provides that an entity is not liable to any proceedings for contravening a secrecy provision in respect of a use or disclosure of personal information authorised by s 80P(1), unless the secrecy provision is a 'designated secrecy provision'. Designated secrecy provisions include provisions under the *Australian Security Intelligence Organisation Act 1979* (Cth) and the *Intelligence Services Act 2001* (Cth).[68]

ALRC Privacy Inquiry

7.43 In *For Your Information: Australian Privacy Law and Practice* (ALRC 108), the ALRC considered whether secrecy provisions in federal legislation contribute to inconsistency and fragmentation in the regulation of personal information. The ALRC also considered whether there is a need to clarify the relationship between the *Privacy Act* and other legislation containing secrecy provisions. Unfortunately, relatively few stakeholders made submissions on these issues.[69]

7.44 The ALRC concluded that, for a number of reasons, it is appropriate that specific laws, rather than the *Privacy Act,* include secrecy provisions designed to protect information. First, inserting criminal offences into the *Privacy Act* would be inconsistent with the 'light touch' regulatory regime for privacy. It would not be

64 Ibid, s 44.
65 Ibid, s 45.
66 Ibid, s 55A.
67 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.
68 *Privacy Act 1988* (Cth), s 80P(7).
69 Nearly 600 submissions were received over the course of the ALRC's Privacy Inquiry. Only 6 stakeholders commented on secrecy in response to Australian Law Reform Commission, *Review of Privacy*, Issues Paper 31 (2006). No stakeholder addressed the issue in response to Australian Law Reform Commission, *Review of Australian Privacy Law*, Discussion Paper 72 (2007). Those stakeholders that commented on the earlier stages were: Australian Government Department of Employment and Workplace Relations, Australian Bureau of Statistics, the Australian Government Department of Health and Ageing, Office of the Victorian Privacy Commissioner, Office of the Privacy Commissioner and Australian Privacy Foundation. See Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [15.116].

appropriate for the privacy regulator, the Federal Privacy Commissioner, to administer and enforce secrecy provisions.[70] Secondly, as discussed in Chapter 2:

> Secrecy provisions do not relate solely to personal information. They also protect, for example, commercial, security and operational information. Secrecy provisions provide separate and specific standards of protection beyond those afforded by the privacy principles … Unlike the privacy principles, the level of protection afforded by secrecy provisions will often vary with the sensitivity of the information concerned.[71]

7.45 Given that secrecy provisions may adversely affect the privacy of an individual, however, the ALRC suggested that a privacy impact assessment should be prepared when a secrecy provision is proposed that may have a significant impact on the handling of personal information. Further, the ALRC suggested that where a secrecy provision regulates personal information, that provision should address how the requirements under the provision interact with the privacy principles in the *Privacy Act.*[72]

Should secrecy provisions regulate personal information?

7.46 In cases where both the *Privacy Act* and a secrecy provision regulate handling of personal information, there may be an issue about whether this overlap contributes to inconsistency and fragmentation in the regulation of personal information. Further, there may be an issue about whether it is appropriate that unauthorised handling of personal information could give rise both to a requirement for an agency or organisation to pay compensation under the *Privacy Act,* and for criminal or administrative liability under a secrecy provision to fall upon the person or body that disclosed it.

7.47 For example, s 16 of the *Customs Administration Act 1985* (Cth) restricts the handling of 'protected information' unless certain exceptions apply.[73] In addition, if the 'protected information' also contains personal information, then it cannot be disclosed without the consent of the person to whom the personal information relates, or unless the disclosure is made for a permissible purpose set out in s 16(9) and the Chief Executive Officer of the Australian Customs Service is satisfied that the disclosure is necessary for such a purpose.[74] The permissible purposes set out in s 16(9) are very similar to the permitted disclosures set out in the privacy principles dealing with use and disclosure.[75] However, the penalty for contravention of s 16 of the *Customs Administration Act* is two years imprisonment. In contrast, a breach of the relevant privacy principle[76] could result in the Privacy Commissioner making a determination

---

70 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), [15.117]–[15.118].
71 Ibid, [15.121].
72 Ibid, [15.122]–[15.124].
73 These exceptions are set out in *Customs Administration Act 1985* (Cth) ss 3, 3A–3H.
74 See also Ibid s 16(8).
75 See sch 3, NPP 2.
76 *Privacy Act 1988* (Cth) sch 3, NPP 2; s 14, IPP 11.

that a complainant is entitled to a compensation payment for any loss or damage suffered.[77]

7.48 The ALRC is interested in hearing about the impact of the overlap in regulation of personal information. In this Inquiry, the ALRC is interested in hearing stakeholder views on whether secrecy provisions should regulate personal information, or whether this information should be regulated exclusively through the *Privacy Act.*

Terminology

7.49 If secrecy provisions should regulate personal information, an issue is whether the overlap in regulation should be clarified. In this section, the ALRC considers the terminology used in secrecy provisions in the privacy context.[78]

7.50 Some secrecy provisions, such as s 86–2(1) of the *Aged Care Act 1997* (Cth)*,* refer to personal information. That Act defines personal information in identical terms to the *Privacy Act,* but without reference to the *Privacy Act*.[79] As noted above, s 16 of the *Customs Administration Act* also regulates the handling of 'protected information', which may include personal information. In that Act, however, personal information is expressly defined as having the same meaning as that set out in the *Privacy Act*.[80]

7.51 A variety of formulations are used in other provisions. For example, s 30 of the *A New Tax System (Australian Business Number) Act 1999* (Cth) sets out what an 'entrusted person' must not do with 'protected information' obtained in the course of official employment. Protected information is defined to include information that 'relates to the affairs of a person other than the entrusted person'.[81]

7.52 Section 193S of the *Aboriginal and Torres Strait Islander Act 2005* (Cth) regulates the handling by an Indigenous Land Corporation (ILC) officer of 'any information concerning the affairs of another person' that was acquired by the ILC officer.[82] Further, s 193S regulates the handling of 'any information' acquired by the ILC officer where he or she is aware that 'the information is considered sacred or

---

77 Ibid s 52(1)(iii).

78 Terminology used in secrecy provisions is also discussed in Ch 2.

79 *Aged Care Act 1997* (Cth) sch 3.

80 *Customs Administration Act 1985* (Cth) s 16(1A), 16(7).

81 *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.

82 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3)(a). *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3) regulates the disclosure of information that was acquired by an ILC officer in connection with an application for, or the giving of, a loan, grant or guarantee; or the disclosure of the information could reasonably be expected to prejudice substantially the commercial interests of the other person.

otherwise significant by a particular group of Aboriginal persons or Torres Strait Islanders', and such disclosure 'would be inconsistent with the views or sensitivities' of these peoples.[83]

7.53 Another example is contained in s 16 of the *Income Tax Assessment Act 1936* (Cth). This provision prevents the disclosure by an officer of 'any information respecting the affairs of another person' that was acquired by reason of that officer's employment or appointment, or in the course of employment, by the Commonwealth or a State.[84] The section also contains an exception for disclosure in the performance of the person's duties as an officer.[85] However, this exception may not apply, for example, to an officer who uses information that relates to an employee for an internal disciplinary proceeding.[86]

7.54 Australian courts have considered the meaning of 'personal affairs' in a number of cases. 'Personal affairs' is generally considered to be a different concept than 'personal information'. For example, in *Young v Wicks*, 'personal affairs' was interpreted as 'matters of private concern to a person'.[87] Rather than the nature of the information, however, what is critical to the definition of 'personal information' under the *Privacy Act* is that the information is capable of identifying an individual. Under the current definition of 'personal information',[88] if an individual's identity is clear, or reasonably capable of being ascertained, then any information about him or her is covered, whether or not it is of private concern.

7.55 In the context of secrecy provisions, the *Acts Interpretation Act 1901* (Cth) provides that the word 'person' includes a body politic or corporate as well as an individual.[89] 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.

---

83 *Aboriginal and Torres Strait Islander Act 2005* (Cth) s 193S(3)(b). In ALRC 108, the ALRC was not of the view that the *Privacy Act 1988* (Cth) should be extended to regulate the information of Indigenous groups: Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008) Rec 7–1.

84 *Income Tax Assessment Act 1936* (Cth) s 16(2). An officer is defined in s 16(1). The provision also applies to persons who perform services for the Commonwealth: s 16(1A).

85 Ibid s 16(2A). See also discussion of the intersection between s 16 of the *Income Tax Assessment Act 1936* (Cth) and *Privacy Act 1988* (Cth) s 14, IPP 11.1(e) in M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt I)' (2002) 8 *Privacy Law & Policy Reporter* 181; M McLennan, 'Negotiating Secrecy and Privacy Issues in Government (Pt II)' (2002) 8 *Privacy Law & Policy Reporter* 193.

86 The role of the Commissioner of Taxation as both an employer and the head of a government agency is discussed in the context of information flows in Ch 1.

87 *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.

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

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

7.56 If secrecy provisions should regulate personal information, the ALRC is interested in hearing whether these provisions should refer to, or use the same terminology as the *Privacy Act*.

Access and correction rights

7.57 As noted above, the *Privacy Act* provides individuals with access and correction rights for personal information that relates to them, unless denying access is required or authorised by or under law.[90] If secrecy provisions should regulate personal information, there may be an issue whether they should restrict disclosure of that information to the individual about whom the information relates.

7.58 Currently, secrecy provisions take various approaches to this issue. Section 86–2 of the *Aged Care Act* creates an offence for the unauthorised handling of 'protected information' acquired by the person in the course of performing duties or exercising powers or functions under the Act. However, the section contains an exception for information disclosed 'only to the person to whom it relates'.[91]

7.59 Section 94 of the *Australian Trade Commission Act 1985* (Cth) restricts the disclosure of information by a person, to any person, of 'any information concerning the affairs of another person acquired by the first-mentioned person by reason of his or her employment'. While this provision does not contain an exception that expressly allows the disclosure of information to an individual to whom the information relates, it appears from the wording of the provision that such disclosure would be permitted.

7.60 In contrast, s 44 of the *Surveillance Devices Act 2004* (Cth) does not allow the disclosure to an individual of personal information about that individual. This section creates two offences for the disclosure of 'protected information'.[92] Protected information is defined to include 'any information that is likely to enable the identification of a person, object or premises specified in a warrant'. This could include personal information. Section 44 sets out a number of exceptions to these offences—however, there is no exception that is equivalent to that contained in s 86–2 of the *Aged Care Act.*

7.61 The ALRC is interested in hearing whether, if secrecy provisions should regulate personal information, these provisions should allow individuals to access and correct personal information about themselves.

---

90 *Privacy Act 1988* (Cth), s 14, IPP 6; sch 3, NPP 6.1(h).

91 *Aged Care Act 1997* (Cth) s 86–2(2)(b).

92 *Surveillance Devices Act 2004* (Cth) s 44(3) also prohibits the admission of protected information in evidence in any proceedings.

Facilitating disclosure?

7.62 The *Privacy Act* and some secrecy provisions place restrictions around the handling of personal information. However, there may be an issue where a secrecy provision facilitates disclosure of personal information by triggering exceptions in the privacy principles. This could occur if a secrecy provision contains an exception to the prohibition on disclosure. Exceptions in secrecy provisions often mirror the exceptions set out in the privacy principles. However, if a secrecy provision contains an exception that is not contained in the privacy principles, this could allow disclosure of personal information that would otherwise be a breach of the privacy principles.

7.63 Such an exception in a secrecy provision would be consistent with the *Privacy Act* because it could fall within two types of exceptions in the privacy principles. First, use and disclosure is permitted under the privacy principles if this is 'required or authorised by or under law'.[93] Secondly, use and disclosure is also permitted under the privacy principles if this is 'reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue'.[94]

7.64 The ALRC is interested in hearing whether there are situations in which it is appropriate for secrecy provisions to authorise handling of personal information where that handling would otherwise be in breach of the *Privacy Act.*

Question 7–4 Does the relationship between secrecy provisions and the *Privacy Act 1988* (Cth) need to be clarified? In particular, should secrecy provisions regulate personal information? If so, should secrecy provisions:

(a) refer to, or use the terminology of, the *Privacy Act*?

(b) allow individuals to access and correct personal information about themselves?

Question 7–5 In what situations is it appropriate for secrecy provisions to authorise handling of personal information where that handling would otherwise breach the *Privacy Act 1988* (Cth)?

93 *Privacy Act 1988* (Cth) s 14, IPPs 10.1(c) and 11.1(d); sch 3, NPP 2.1(g).
94 Ibid s 14, IPPs 10.1(d) and 11.1(e); sch 3, NPP 2.1(h).

Data-matching

7.65 Data-matching is 'the large scale comparison of records or files … collected or held for different purposes, with a view to identifying matters of interest'.[95] Agencies and organisations may wish to conduct data-matching for a number of reasons. Data-matching can be conducted for a number of purposes, including detecting errors and illegal behaviour, locating individuals, ascertaining whether a particular individual is eligible to receive a benefit, and facilitating debt collection.[96]

Overview of data-matching regulation

7.66 Agencies wishing to undertake data-matching activities may be prevented from carrying out these activities by secrecy provisions that prevent Commonwealth officers from using or disclosing relevant information.

7.67 Agencies and organisations are subject to additional forms of regulation in respect of their data-matching activities. Information-handling requirements in the privacy principles apply to agencies and organisations that undertake data-matching activities.[97] Further, agencies undertaking data-matching programs that include the matching of tax file numbers are subject to the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) and the *Data-matching Program (Assistance and Tax) Guidelines* issued under that Act.

7.68 Finally, the Federal Privacy Commissioner has functions related to data-matching. These include undertaking research and monitoring developments in data processing and computer technology (including data-matching and data linkage) to help minimise any adverse effects of such developments on privacy.[98]

7.69 The Federal Privacy Commissioner has issued voluntary guidelines that address general data-matching activities of agencies and a number of agencies have agreed to comply with them.[99] The guidelines apply to agencies that match data from two or more databases, if at least two of the databases contain information about more than

---

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

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

97 *Privacy Act 1988* (Cth) s 14, IPP 10 and 11 and *Privacy Act 1988* (Cth) Sch 3, NPPs 2 and 10.

98 *Privacy Act 1988* (Cth) s 27(1)(c). In addition, the Federal Privacy Commissioner can examine (with or without a request from a minister) any proposal for data-matching or data linkage that may involve an interference with privacy or that may have any adverse effects on the privacy of individuals. The Federal Privacy Commissioner may report to the minister responsible for administering the *Privacy Act* about the results of any research into developments in data-matching or proposals for data-matching: *Privacy Act 1988* (Cth) ss 27(1)(c), 32(1).

99 In 2007–2008, the Federal Privacy Commissioner was provided with agency protocols for 13 data-matching programs: Office of the Federal Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2007–30 June 2008* (2008) 64–71.

5,000 individuals.[100] In summary, the guidelines require agencies to: give public notice of any proposed data-matching program; prepare and publish a 'program protocol' outlining the nature and scope of a data-matching program; provide individuals with an opportunity to comment on matched information if the agency proposes to take administrative action on the basis of it; and destroy personal information that does not lead to a match. Further, the voluntary data-matching guidelines generally prohibit agencies from creating new, separate databases from information about individuals whose records have been matched.[101]

Interaction between secrecy provisions and data-matching

7.70 One issue is whether secrecy provisions inappropriately restrict information-sharing between agencies. Data-matching may assist an agency to establish or verify an individual's identity to facilitate that individual's enrolment in an electronic system. Secrecy provisions could prevent data-matching conducted for the purpose of detecting errors and identity fraud in existing systems.[102]

7.71 Increasingly, federal, state and territory governments are focusing on issues related to identity security. Since April 2005, the Australian Government Attorney-General's Department has been developing and implementing a National Identity Security Strategy (NISS), which comprises the national Document Verification Service and the e-Authentication framework.[103]

7.72 There are a number of obvious privacy risks associated with data-matching. In the voluntary guidelines, the Federal Privacy Commissioner notes that data-matching may involve the:

- use of personal information for purposes other than for the reasons it was collected, and these purposes may not be within the reasonable expectations of the individuals about whom the personal information relates;

---

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

101 Ibid, [33]–[41], [42]–[47], [63], [69]. In Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008), the ALRC suggested that the Office of the Privacy Commissioner could exercise its research and monitoring function to review the voluntary 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.

102 The issue of whether secrecy provisions generally hinder information flows between Government agencies, and between agencies and the private sector, is considered in Ch 1.

103 See, eg, Council of Australian Governments (COAG), *Intergovernmental Agreement to a National Identity Security Strategy*, 13 April 2007; National Identity Security Coordination Group, *Report to the Council of Australian Governments on the Elements of the National Identity Security Strategy* (2007); Australian Government Attorney-General's Department, *Identity Security—National Document Verification Service (DVS)* (2008) <http://www.ag.gov.au/www/agd/agd.nsf/Page/Crimeprevention_Identitysecurity#q1> at 4 November 2008; Australian Government Department of Finance and Deregulation, *Australian Government e Authentication Framework for Individuals* (2008) <http://www.finance.gov.au/e-government/security-and-authentication/agaf-i.html> at 4 November 2008.

- examination of personal information about individuals about whom there are no grounds for suspicion, sometimes without the knowledge of those individuals; and

- retention of matched information by agencies for potential future use.[104]

7.73 The Federal Privacy Commissioner also notes that data-matching is not always reliable. Matched information may fail to distinguish between individuals with similar details; input data may not be accurate; technical errors may occur; and fields may not be standardised.[105]

7.74 Some data-matching activities of agencies may fall within exceptions in secrecy provisions. For example, s 130 of the *Health Insurance Act 1973* (Cth) provides that information only may be disclosed for the purposes of that Act, but the minister responsible for administering the Act may authorise disclosure if it is necessary in the public interest to disclose it, or if the disclosure is in accordance with a purpose, person or authority prescribed in regulations.

7.75 The Terms of Reference for this Inquiry require the ALRC to have regard to the increased need to share information within and between governments and the private sector, and in Chapter 1, the ALRC asked for information about the impact of secrecy provisions in this context.[106] The ALRC is also interested in hearing about whether secrecy provisions may be inappropriately inhibiting information sharing between agencies through data-matching. If it is necessary to address this issue, what is the best approach? For example, should facilitative clauses permit data-matching conducted for particular purposes? If so, what should be the limits on such clauses?

Question 7–6 What concerns arise from the interaction between secrecy provisions and data-matching laws and practices? How should these issues be addressed?

104 Office of the Federal Privacy Commissioner, *The Use of Data-Matching in Commonwealth Administration—Guidelines* (1998), 2.
105 Ibid, 2.
106 Question 1–2.

Archives

Overview of the *Archives Act*

7.76 The FOI Act and the *Archives Act* were both introduced as part of a package of administrative law reforms in the early 1980s. Both Acts deal with access to documents and records, and are interconnected.

7.77 The *Archives Act* established the National Archives of Australia (NAA) and set out comprehensive arrangements for conserving and preserving the archival resources of the Commonwealth.[107] It also established a right of access to Commonwealth records that have been in existence for more than 30 years. This is described as the 'open access period'.[108] Documents less than 30 years old may be released in special circumstances.[109]

7.78 As noted in ALRC 77, the role of the NAA includes

> encouraging and facilitating the use of archives, developing policy and advice for government agencies on the management, preservation and disposal of records and creating and maintaining information systems about the structure of government and the Commonwealth's record series.[110]

7.79 The NAA is responsible for providing public access to government records that are more than 30 years old. Where classified records are transferred to the NAA, they retain their classification and are stored and handled accordingly. However, the fact that, for example, a record is classified does not mean that it is automatically exempt, and all records are assessed on a case-by-case basis. Where a security classified record is released under the Act, the classification ceases to have effect.[111] The NAA encourages agencies to declassify records, wherever possible, before transferring them to the NAA.[112]

Interaction between secrecy provisions and the *Archives Act*

7.80 The *Archives Act* does contain some exemptions for access to records in the open access period, but these exemptions are less restrictive than those under the FOI

---

107 *Archives Act 1983* (Cth) pt V.

108 Ibid s 31. Cabinet notebooks are in the open access period after they have been in existence for 50 years, and records containing census information are in the open access period after they have been in existence for 99 years: *Archives Act 1983* (Cth) ss 22A, 22B. The Act creates an offence for disclosure of census information that is not in the open access period: s 30A. Census information is discussed further in Ch 2.

109 *Archives Act 1983* (Cth) s 56. In addition, the *Archives Act* does not prevent a person from giving access to records (including exempt records) not in pursuance with the Act, where this is required or authorised by law: Ibid, s 58.

110 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].

111 *Archives Act 1983* (Cth) s 59.

112 In 2004, the ALRC recommended that all Australian Government agencies review classified information with a view to declassification or reclassification in a number of specified circumstances, including before transfer to the NAA: Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information*, ALRC 98 (2004), Rec 4–7.

Act because the records sought are older and generally less sensitive. The *Archives Act* does not contain a specific exemption preventing access to records that contain information that is the subject of a secrecy provision. However, information or documents that are subject to secrecy provisions may fall within a number of exemptions set out in the *Archives Act*.

7.81 Certain Commonwealth records do not need to be disclosed by the NAA even if they fall within the open access period. For example, records that contain 'information or matter' do not need to be disclosed if they:

- could reasonably be expected to cause damage to the security, defence or international relations of the Commonwealth;
- would have a substantial adverse effect on the financial or property interests of the Commonwealth or of a Commonwealth institution and would not, on balance, be in the public interest;
- would constitute a breach of confidence;
- would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person); or
- would, or could reasonably be expected to, destroy or diminish trade secrets or any other matter having a commercial value if it were disclosed.[113]

7.82 In the 1998 Report, *Australia's Federal Record: A Review of Archives Act 1983* (ALRC 85), the ALRC considered exemptions in the *Archives Act.* The ALRC recommended that the number of categories for exempt documents be reduced. The ALRC also recommended that the Act should be amended to include an exemption category relating to information that, under Indigenous tradition, is confidential or subject to particular disclosure restrictions.[114]

113 Other exemptions are set out in the *Archives Act 1983* (Cth) s 33.

114 Australian Law Reform Commission, *Australia's Federal Record: A Review of the Archives Act 1983*, ALRC 85 (1998), Rec 164. The ALRC recommended that the language of this category should be consistent with that of the exemption proposed in the Aboriginal and Torres Strait Islander Heritage Protection Bill 1998. The ALRC also recommended that a similar exemption be included in the FOI Act: Ibid, Rec 165.

7.83 On 1 November 2008, the *Archives Amendment Act 2008* (Cth) came into operation. This Act implements several of the recommendations made by the ALRC in ALRC 85, but the Act does not remove any exemptions from the *Archives Act.*[115]

7.84 The ALRC is interested in hearing about how the relationship between secrecy provisions and the *Archives Act* is working in practice, and if there are any concerns, how these should be addressed.

Question 7–7 Does the relationship between secrecy provisions and the *Archives Act 1983* (Cth) need to be clarified? If so, how?

Other issues

7.85 The ALRC is interested in hearing whether there may be any other concerns about the interaction of secrecy provisions with other legislation regulating the handling of Commonwealth information.

Question 7–8 Are there any other concerns about the interaction of secrecy provisions with other legislation regulating the handling of Commonwealth information?

115 The *Archives Amendment Act 2008* (Cth) inserts an objects clause into the *Archives Act 1983* (Cth), and makes changes to ensure that records remain in the 'care' of the NAA when in custody of persons other than the NAA.

Appendix 1. List of Abbreviations

AAT	Administrative Appeals Tribunal
ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
ADF	Australian Defence Force
ADJR Act	*Administrative Decisions (Judicial Review) Act 1977* (Cth)
AEC	Australian Electoral Commission
AFP	Australian Federal Police
AFP Act	*Australian Federal Police Act 1979* (Cth)
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,* ALRC 77 (1995)
ALRC 85	Australian Law Reform Commission, *Australia's Federal Record: A Review of Archives Act 1983,* ALRC 85 (1998)
ALRC 98	Australian Law Reform Commission, *Keeping Secrets: The Protection of Classified and Security Sensitive Information,* ALRC 98 (2004)
ALRC 108	Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108 (2008)

ALRC 102	Australian Law Reform Commission, New South Wales Law Reform Commission and Victorian Law Reform Commission, *Uniform Evidence Law*, ALRC 102 (2005)
AMC	Australian Military Court
ANAO	Australian National Audit Office
APS	Australian Public Service
APSC	Australian Public Service Commission
ARC	Administrative Review Council
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
ASIS	Australian Secret Intelligence Service
ATO	Australian Taxation Office
CCPM	Case Categorisation and Prioritisation Model
CDPP	Commonwealth Director of Public Prosecutions
CO	Commanding Officer
COAG	Council of Australian Governments
DFD Act	*Defence Force Discipline Act 1982* (Cth)
DFO	Defence Force Ombudsman
DIGO	Defence Imagery and Geospatial Organisation
DIO	Defence Intelligence Organisation
DPP	Director of Public Prosecutions
DSD	Defence Signals Directorate

FOI	Freedom of Information
FOI Act	*Freedom of Information Act 1982* (Cth)
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and communication technology
IGADF	Inspector-General of the Australian Defence Force
IGIS	Inspector-General of Intelligence and Security
ILC	Indigenous Land Corporation
IPPs	Information Privacy Principles
MOU	Memorandum of understanding
MPC	Merit Protection Commissioner
NAA	National Archives of Australia
NCIDD	National Criminal Investigation DNA Database
NISS	National Identity Security Strategy
NPPs	National Privacy Principles
ONA	Office of National Assessments
Privacy Act	*Privacy Act 1988* (Cth)
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PSCC	Protective Security Coordination Centre, Attorney-General's Department
PSM	Australian Government Protective Security Manual

Senate Committee Inquiry	Senate Legal and Constitutional Affairs Committee, *Inquiry into the Freedom of Information Amendment (Open Government) Bill 2000*
Taxation Secrecy Review	Australian Government—The Treasury, *Review of Taxation Secrecy and Disclosure Provisions*: Discussion Paper (2006)
UK	United Kingdom
US	United States

Appendix 2. Table of Secrecy Provisions

This table lists provisions in Commonwealth legislation that impose secrecy or confidentiality obligations, as identified to date. Provisions that deal only with exceptions to such secrecy or confidentiality obligations and other associated or ancillary matters are not included.

Legislation	**Provision**
A New Tax System (Australian Business Number) Act 1999	ss 26, 30
A New Tax System (Bonuses for Older Australians) Act 1999	s 55
A New Tax System (Family Assistance) (Administration) Act 1999	ss 163, 164, 165, 166
A New Tax System (Goods and Services Tax Administration) Act 1999	s 68
Aboriginal and Torres Strait Islander Act 2005	ss 191, 193S, 200A
Aboriginal Land Rights (Northern Territory) Act 1976	s 23E
Age Discrimination Act 2004	s 60
Aged Care Act 1997	ss 62-1, 63-1AA, 86-2, 86-5, 86-6, 86-7
Agricultural and Veterinary Chemicals Code Act 1994	s 162
Agricultural and Veterinary Chemicals Code Regulations 1995	reg 69
Air Navigation (Confidential Reporting) Regulations 2006	reg 14

Legislation	Provision
Air Navigation Regulations 1947	reg 12
Airports (Building Control) Regulations 1996	reg 4.03
Airports (Environment Protection) Regulations 1997	reg 10.06
Anti-Money Laundering and Counter-Terrorism Financing Act 2006	ss 121, 122, 123, 127, 128, 130, 131
Archives Act 1983	s 30A
Auditor-General Act 1997	ss 36, 37
AusCheck Act 2007	s 15
Australian Citizenship Act 2007	ss 42, 43
Australian Crime Commission Act 2002	ss 9, 29B, 51
Australian Federal Police Act 1979	ss 40ZA, 60A
Australian Federal Police Regulations 1979	regs 12, 13B, 13C
Australian Hearing Services Act 1991	s 67
Australian Institute of Aboriginal and Torres Strait Islander Studies Act 1989	s 41
Australian Institute of Health and Welfare Act 1987	s 29
Australian Postal Corporation Act 1989	ss 90H, 90LB, 90LE
Australian Prudential Regulation Authority Act 1998	s 56
Australian Securities and Investments Commission Act 2001	ss 127, 213, 237

Legislation	**Provision**
Australian Security Intelligence Organisation Act 1979	ss 18, 34ZS, 81, 92
Australian Sports Anti-Doping Authority Act 2006	ss 71, 72
Australian Trade Commission Act 1985	s 94
Australian Wine and Brandy Corporation (Annual General Meeting of the Industry) Regulations 1999	reg 9
Aviation Transport Security Act 2004	s 74
Aviation Transport Security Regulations 2005	regs 2.06, 4.46
Banking Act 1959	ss 11CF, 52E
Bankruptcy Regulations 1996	regs 8.05O, 8.32
Broadcasting Services (Transitional Provisions and Consequential Amendments) Act 1992	s 25
Building and Construction Industry Improvement Act 2005	ss 65, 66
Cadet Forces Regulations 1977	sch 4, cl 5
Census and Statistics Act 1905	ss 12, 13, 19, 19A
Chemical Weapons (Prohibition) Act 1994	s 102
Child Care Act 1972	ss 12K, 12L, 12Q, 12R, 12S
Child Support (Assessment) Act 1989	ss 150, 150AA

Legislation	Provision
Child Support (Registration and Collection) Act 1988	ss 16, 16AA, 58
Civil Aviation Act 1988	s 32AP
Civil Aviation Regulations 1988	reg 132
Coal Mining Industry (Long Service Leave) Payroll Levy Collection Act 1992	s 14
Commonwealth Electoral Act 1918	ss 90B, 91A, 91B, 189B, 323
Commonwealth Functions (Statutes Review) Act 1981	s 234
Competition Policy Reform (Transitional Provisions) Regulations 1995	reg 6
Comprehensive Nuclear Test Ban Treaty Act 1998	s 74
Copyright Act 1968	s 203E
Corporations (Aboriginal and Torres Strait Islander) Act 2006	ss 175-10, 183-1, 472-1, 604-15, 604-20
Crimes Act 1914	ss 3ZQJ, 3ZQT, 15XS, 23XG, 23XWO, 23YO, 70, 79, 83
Criminal Code	ss 91.1, 105.41
Customs Act 1901	s 64ADA
Customs Administration Act 1985	s 16
Dairy Produce Act 1986	ss 119, sch 2, cl 43
Data-matching Program (Assistance and Tax) Act 1990	s 15
Defence Act 1903	s 73A
Defence (Inquiry) Regulations 1985	regs 62, 63

Legislation	**Provision**
Defence Force Discipline Act 1982	ss 16, 58
Defence (Special Undertakings) Act 1952	s 9
Dental Benefits Act 2008	ss 34, 43, 44, 45, 46
Designs Act 2003	ss 61, 108
Development Allowance Authority Act 1992	s 114
Disability Discrimination Act 1992	s 127
Disability Services Act 1986	s 28
Environment Protection (Alligator Rivers Region) Act 1978	s 31
Environment Protection and Biodiversity Conservation Act 1999	s 390R
Epidemiological Studies (Confidentiality) Act 1981	ss 4, 6
Excise Act 1901	s 159
Export Finance and Insurance Corporation Act 1991	s 87
Family Law Act 1975	ss 10D, 10H
Financial Transaction Reports Act 1988	s 16
Film Licensed Investment Company (Application) Rules 2005	r 17
Financial Management and Accountability Regulations 1997	Notes, Table A, item 6
First Home Saver Accounts Act 2008	s 70

Legislation	Provision
Fisheries Management Act 1991	sch 1A, cl 53
Fisheries Management Regulations 1992	reg 36
Food Standards Australia New Zealand Act 1991	s 114
Fringe Benefits Tax Assessment Act 1986	s 5
Gene Technology Act 2000	s 187
Health Insurance Act 1973	ss 124Y, 130
Health Insurance Regulations 1975	reg 23C
Higher Education Funding Act 1988	s 78
Higher Education Support Act 2003	ss 179-10, 179-35
Human Rights and Equal Opportunity Commission Act 1986	ss 24, 49
Income Tax Assessment Act 1936	ss 16, 16A
Income Tax Assessment Act 1997	s 396-95
Industry Research and Development Act 1986	s 47
Inspector-General of Intelligence and Security Act 1986	s 34
Inspector-General of Taxation Act 2003	s 37
Inspector of Transport Security Act 2006	ss 35, 36, 37, 49, 56, 60, 61, 62, 63, 64, 67, 68, 69, 75, 77
Insurance Act 1973	s 107
Intelligence Services Act 2001	ss 39, 39A, 40, 41, sch 1 cl 9
International Criminal Court Act 2002	ss 13, 92

Legislation	**Provision**
Law Enforcement Integrity Commissioner Act 2006	ss 90, 92, 207
Life Insurance Act 1995	ss 156E, 230E
Maritime Transport and Offshore Facilities Securities Act 2003	s 40
Medical Indemnity Act 2002	s 77
Migration Act 1958	ss 46B, 48B, 72, 91F, 91L, 91Q, 91Y, 195A, 197AG, 261AKD, 336C, 336E, 377, 439, 503A
Migration Agents Regulations 1998	sch 2 cls 3.1, 3.2
Military Rehabilitation and Compensation Act 2004	s 409
Mutual Assistance in Criminal Matters Act 1987	ss 34V, 43B, 43C
National Blood Authority Act 2003	s 11
National Health Act 1953	ss 135A, 135AAA
National Health and Medical Research Council Act 1992	ss 78, 80
National Health Regulations 1954	reg 32
National Health Security Act 2007	ss 21, 90
National Water Commission Act 2004	s 43
National Workplace Relations Consultative Council Act 2002	s 5
Nuclear Non-Proliferation (Safeguards) Act 1987	s 71

Legislation	Provision
Occupational Health and Safety (Safety Standards) Regulations 1994	regs 8.61, 9.68
Offshore Minerals Act 1994	s 374
Ombudsman Act 1976	ss 19U, 35
Parliamentary Commission of Inquiry (Repeal) Act 1986	s 7
Patents Act 1990	ss 56, 173, 183, 184
Petroleum Resource Rent Tax Assessment Act 1987	ss 17, 18
Pooled Development Funds Act 1992	s 71
Port Statistics Act 1977	s 7
Postal and Telecommunications Commissions (Transitional Provisions) Act 1975	s 37
Privacy Act 1988	ss 70, 80Q, 96
Privacy (Private Sector) Regulations 2001	sch 1 cl 4.6
Private Health Insurance Act 2007	ss 323–1, 323–40, 323–45, 323–50, 323–55
Proceeds of Crime Act 1987	s 74
Proceeds of Crime Act 2002	ss 210, 217, 223
Product Grants and Benefits Administration Act 2000	s 47
Productivity Commission Act 1998	s 53
Public Service Act 1999	s 13
Public Service Regulations 1999	regs 2.1, 6.3, 7.6

Legislation	**Provision**
Racial Discrimination Act 1975	s 27F
Referendum (Machinery Provisions) Act 1984	s 116
Renewable Energy (Electricity) Act 2000	s 127
Research Involving Human Embryos Act 2002	ss 29, 30
Reserve Bank Act 1959	ss 79A, 79B
Sex Discrimination Act 1984	ss 92, 112
Social Security (Administration) Act 1999	ss 203, 204, 205, 206
Social Welfare Commission (Repeal) Act 1976	s 8
Space Activities Act 1998	s 96
Student Assistance Act 1973	ss 12ZU, 352, 353, 357, 358, 359
Superannuation (Government Co-contribution for Low Income Earners) Act 2003	s 53
Superannuation (Resolution of Complaints) Act 1993	s 63
Superannuation (Unclaimed Money and Lost Members) Act 1999	s 32
Superannuation Contributions Tax (Assessment and Collection) Act 1997	s 32
Superannuation Contributions Tax (Members of Constitutionally Protected Superannuation Funds) Assessment and Collection Act 1997	s 28

Legislation	Provision
Superannuation Guarantee (Administration) Act 1992	s 45
Superannuation Industry (Supervision) Act 1993	s 252C
Surveillance Devices Act 2004	s 45
Taxation Administration Act 1953	ss 3C, 3D, 3E, 3EA, 3EB, 3EC, 3G, 3H, 8WB, 8XA, 8XB, 13H, 13J, sch 1 s 355-5
Taxation (Interests on Overpayments and Early Payments) Act 1983	s 8
Telecommunications (Consumer Protection and Service Standards) Act 1999	ss 22, 22A
Telecommunications (Interception and Access) Act 1979	ss 63, 133, 182, 202
Termination Payments Tax (Assessment and Collection) Act 1997	s 23
Therapeutic Goods Act 1989	s 9C
Torres Strait Fisheries Act 1984	sch 2 cls 51, 53
Torres Strait Fisheries Regulations 1985	reg 13
Trade Marks Act 1995	ss 226A, 258
Trade Practices Act 1974	ss 44AAF, 89, 95, 95AI, 95AZA, 95ZN, 95ZP, 95ZQ, 10.37, 10.88, 10.89, 152AYA
Trade Practices Regulations 1974	reg 7D
Transport Safety Investigation Act 2003	ss 26, 53, 60
Veterans' Entitlements Act 1986	ss 34, 35H, 36L, 37L, 38L, 45Q, 57E, 79I, 93ZE, 116D, 118ZF, 118ZX, 137, 140, 153, 196ZD

Legislation	**Provision**
Water Act 2007	s 215
Wheat Export Marketing Act 2008	s 74
Witness Protection Act 1994	ss 16, 22
Workplace Relations Act 1996	ss 163C, 165, 166T, 425, 485, 486, 702, 707, 712, 715, sch 1 cl 276

Appendix 3. Extracts of Key Secrecy Provisions

Contents

The following extracts include some of the principal provisions referred to in the text of this Issues Paper. Provisions referred to in passing only, or otherwise adequately set out in the text, are not included in this Appendix.

Crimes Act 1914 (Cth)

Section 70–Disclosure of information by Commonwealth officers

(1) A person who, being a Commonwealth officer, publishes or communicates, except to some person to whom he or she is authorized to publish or communicate it, any fact or document which comes to his or her knowledge, or into his or her possession, by virtue of being a Commonwealth officer, and which it is his or her duty not to disclose, shall be guilty of an offence.

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

Penalty: Imprisonment for 2 years.

Section 79–Official secrets

(1) For the purposes of this section, a sketch, plan, photograph, model, cipher, note, document, or article is a prescribed sketch, plan, photograph, model, cipher, note, document or article in relation to a person, and information is prescribed information in relation to a person, if the person has it in his or her possession or control and:

(a) it has been made or obtained in contravention of this Part or in contravention of section 91.1 of the *Criminal Code*;

(b) it has been entrusted to the person by a Commonwealth officer or a person holding office under the Queen or he or she has made or obtained it owing to his or her position as a person:

(i) who is or has been a Commonwealth officer;

(ii) who holds or has held office under the Queen;

(iii) who holds or has held a contract made on behalf of the Queen or the Commonwealth;

(iv) who is or has been employed by or under a person to whom a preceding subparagraph applies; or

(v) acting with the permission of a Minister;

and, by reason of its nature or the circumstances under which it was entrusted to him or her it was made or obtained by him or her or for any other reason, it is his or her duty to treat it as secret; or

(c) it relates to a prohibited place or anything in a prohibited place and:

(i) he or she knows; or

(ii) by reason of its nature or the circumstances under which it came into his or her possession or control or for any other reason, he or she ought to know;

that it should not be communicated to a person not authorized to receive it.

(2) If a person with the intention of prejudicing the security or defence of the Commonwealth or a part of the Queen's dominions:

(a) communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, to a person, other than:

(i) a person to whom he or she is authorized to communicate it; or

(ii) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it;

or permits a person, other than a person referred to in subparagraph (i) or (ii), to have access to it;

(b) retains a prescribed sketch, plan, photograph, model, cipher, note, document or article in his or her possession or control when he or she has no right to retain it or when it is contrary to his or her duty to retain it; or

(c) fails to comply with a direction given by lawful authority with respect to the retention or disposal of a prescribed sketch, plan, photograph, model, cipher, note, document or article;

he or she shall be guilty of an indictable offence.

Penalty: Imprisonment for 7 years.

(3) If a person communicates a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, to a person, other than:

(a) a person to whom he or she is authorized to communicate it; or

(b) a person to whom it is, in the interest of the Commonwealth or a part of the Queen's dominions, his or her duty to communicate it;

or permits a person, other than a person referred to in paragraph (a) or (b), to have access to it, he or she shall be guilty of an offence.

Penalty: Imprisonment for 2 years.

(4) If a person:

(a) retains a prescribed sketch, plan, photograph, model, cipher, note, document or article in his or her possession or control when he or she has no right to retain it or when it is contrary to his or her duty to retain it;

(b) fails to comply with a direction given by lawful authority with respect to the retention or disposal of a prescribed sketch, plan, photograph, model, cipher, note, document or article; or

(c) fails to take reasonable care of a prescribed sketch, plan, photograph, model, cipher, note, document or article, or prescribed information, or to ensure that it is not communicated to a person not authorized to receive it or so conducts himself or herself as to endanger its safety;

he or she shall be guilty of an offence.

Penalty: Imprisonment for 6 months.

(5) If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing or having reasonable ground to believe, at the time when he or she receives it, that it is communicated to him or her in contravention of section 91.1 of the *Criminal Code* or subsection (2) of this section, he or she shall be guilty of an indictable offence unless he or she proves that the communication was contrary to his or her desire.

Penalty: Imprisonment for 7 years.

(6) If a person receives any sketch, plan, photograph, model, cipher, note, document, article or information, knowing, or having reasonable ground to believe, at the time when he or she receives it, that it is communicated to him or her in contravention of subsection (3), he or she shall be guilty of an offence unless he or she proves that the communication was contrary to his or her desire.

Penalty: Imprisonment for 2 years.

(7) On a prosecution under subsection (2) it is not necessary to show that the accused person was guilty of a particular act tending to show an intention to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions and, notwithstanding that such an act is not proved against him or her, he or she may be convicted if, from the circumstances of the case, from his or her conduct or from his or her known character as proved, it appears that his or her intention was to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions.

(8) On a prosecution under this section, evidence is not admissible by virtue of subsection (7) if the magistrate exercising jurisdiction with respect to the examination and commitment for trial of the defendant, or the judge presiding at the trial, as the case may be, is of the opinion that that evidence, if admitted:

(a) would not tend to show that the defendant intended to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions; or

(b) would, having regard to all the circumstances of the case and notwithstanding subsection (9), prejudice the fair trial of the defendant.

(9) If evidence referred to in subsection (8) is admitted at the trial, the judge shall direct the jury that the evidence may be taken into account by the jury only on the question whether the defendant intended to prejudice the security or defence

of the Commonwealth or a part of the Queen's dominions and must be disregarded by the jury in relation to any other question.

(10) A person charged with an offence against subsection (2) may be found guilty of an offence against subsection (3) or (4) and a person charged with an offence against subsection (5) may be found guilty of an offence against subsection (6).

Section 83–Unlawful soundings

(1) Any person who in the Commonwealth or in any Territory:

(a) takes any unlawful soundings;

(b) makes any record of any unlawful soundings;

(c) intentionally has in possession any record of unlawful soundings;

(d) communicates to any person outside the Commonwealth or any Territory any record of or information concerning unlawful soundings; or

(e) communicates to any other person any record of or information concerning unlawful soundings with intent that the record or information may be communicated to any person outside the Commonwealth or any Territory;

shall be guilty of an indictable offence.

Penalty: Imprisonment for 2 years.

(2) For the purposes of this section all soundings taken in the territorial waters of the Commonwealth or any Territory shall be deemed to be unlawful unless they were made under the authority of the Queen, the Commonwealth Government, or a State Government, or the Government of a Territory, or were reasonably necessary for the navigation of the vessel from which they were taken or for any purpose in which the vessel from which they were taken was lawfully engaged.

(3) In any prosecution under this section, proof that any soundings were not unlawfully taken shall lie upon the defendant.

(4) Any figure or word or sign representing a figure (other than the printed figures appearing on any official or recognized map or chart) appearing on any map or sketch of any portion of the coast or territorial waters of Australia or of a Territory shall, in the absence of satisfactory proof to the contrary, be deemed to

be a record of an unlawful sounding, but nothing in this subsection shall affect proof of unlawful soundings in any other manner.

(5) All records of unlawful soundings including all maps or charts having thereon any record of unlawful soundings shall be forfeited to the Commonwealth.

(6) A reference in this section to soundings shall be read as including a reference to a hydrographic survey and a reference to the taking of soundings shall be read as including a reference to the making of a hydrographic survey.

Criminal Code Act 1995 (Cth)

Section 91.1–Espionage and similar activities

(1) A person commits an offence if:

(a) the person communicates, or makes available:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so intending to prejudice the Commonwealth's security or defence; and

(c) the person's act results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation.

Penalty: Imprisonment for 25 years.

(2) A person commits an offence if:

(a) the person communicates, or makes available:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so:

(i) without lawful authority; and

(ii) intending to give an advantage to another country's security or defence; and

(c) the person's act results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation.

Penalty: Imprisonment for 25 years.

(3) A person commits an offence if:

(a) the person makes, obtains or copies a record (in any form) of:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so:

(i) intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation; and

(ii) intending to prejudice the Commonwealth's security or defence.

Penalty: Imprisonment for 25 years.

(4) A person commits an offence if:

(a) the person makes, obtains or copies a record (in any form) of:

(i) information concerning the Commonwealth's security or defence; or

(ii) information concerning the security or defence of another country, being information that the person acquired (whether directly or indirectly) from the Commonwealth; and

(b) the person does so:

(i) without lawful authority; and

(ii) intending that the record will, or may, be delivered to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation; and

(iii) intending to give an advantage to another country's security or defence.

Penalty: Imprisonment for 25 years.

(5) For the purposes of subparagraphs (3)(b)(i) and (4)(b)(ii), the person concerned does not need to have a particular country, foreign organisation or person in mind at the time when the person makes, obtains or copies the record.

(6) A person charged with an offence under this section may only be remanded on bail by a judge of the Supreme Court of a State or Territory. This subsection has effect despite anything in section 93.1.

Note: Section 93.1 deals with how a prosecution is instituted.

(7) Section 15.4 of the *Criminal Code* (extended geographical jurisdiction—category D) applies to offences under this section.

Section 91.2–Defence—information lawfully available

(1) It is a defence to a prosecution of an offence against subsection 91.1(1) or (2) that the information the person communicates or makes available is information that has already been communicated or made available to the public with the authority of the Commonwealth.

(2) It is a defence to a prosecution of an offence against subsection 91.1(3) or (4) that the record of information the person makes, obtains or copies is a record of information that has already been communicated or made available to the public with the authority of the Commonwealth.

Note: A defendant bears an evidential burden in relation to the matters in subsections (1) and (2). See subsection 13.3(3).

Intelligence Services Act 2001 (Cth)

Section 39–Communication of certain information—ASIS

(1) A person is guilty of an offence if:

(a) the person communicates any information or matter that was prepared by or on behalf of ASIS in connection with its functions or relates to the performance by ASIS of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member or agent of ASIS; or

(ii) his or her having entered into any contract, agreement or arrangement with ASIS; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with ASIS; and

(c) the communication was not made:

(i) to the Director-General or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director-General or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member or agent, within the limits of authority conferred on the person by the Director-General; or

(iv) with the approval of the Director-General or of a staff member having the authority of the Director-General to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

Section 39A–Communication of certain information—DIGO

(1) A person commits an offence if:

(a) the person communicates any information or matter that was prepared by or on behalf of DIGO in connection with its functions or relates to the performance by DIGO of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of DIGO; or

(ii) his or her having entered into any contract, agreement or arrangement with DIGO; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DIGO; and

(c) the communication was not made:

(i) to the Director of DIGO or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director of DIGO or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director of DIGO; or

(iv) with the approval of the Director of DIGO or of a staff member having the authority of the Director of DIGO to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

Section 40–Communication of certain information—DSD

(1) A person is guilty of an offence if:

(a) the person communicates any information or matter that was prepared by or on behalf of DSD in connection with its functions or relates to the performance by DSD of its functions; and

(b) the information or matter has come to the knowledge or into the possession of the person by reason of:

(i) his or her being, or having been, a staff member of DSD; or

(ii) his or her having entered into any contract, agreement or arrangement with DSD; or

(iii) his or her having been an employee or agent of a person who has entered into a contract, agreement or arrangement with DSD; and

(c) the communication was not made:

(i) to the Director of DSD or a staff member by the person in the course of the person's duties as a staff member; or

(ii) to the Director of DSD or a staff member by the person in accordance with a contract, agreement or arrangement; or

(iii) by the person in the course of the person's duties as a staff member, within the limits of authority conferred on the person by the Director of DSD; or

(iv) with the approval of the Director of DSD or of a staff member having the authority of the Director of DSD to give such an approval.

Penalty: Imprisonment for 2 years or 120 penalty units, or both.

(2) A prosecution for an offence against subsection (1) may be instituted only by the Attorney-General or with the Attorney-General's consent.

Public Service Regulations 1999 (Cth)

Regulation 2.1–Duty not to disclose information (Act s 13)

(1) This regulation is made for subsection 13(13) of the Act.

(2) This regulation does not affect other restrictions on the disclosure of information.

(3) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if it is reasonably foreseeable that the disclosure could be prejudicial to the effective working of government, including the formulation or implementation of policies or programs.

(4) An APS employee must not disclose information which the APS employee obtains or generates in connection with the APS employee's employment if the information:

(a) was, or is to be, communicated in confidence within the government; or

(b) was received in confidence by the government from a person or persons outside the government;

whether or not the disclosure would found an action for breach of confidence.

(5) Subregulations (3) and (4) do not prevent a disclosure of information by an APS employee if:

(a) the information is disclosed in the course of the APS employee's duties; or

(b) the information is disclosed in accordance with an authorisation given by an Agency Head; or

(c) the disclosure is otherwise authorised by law; or

(d) the information that is disclosed:

(i) is already in the public domain as the result of a disclosure of information that is lawful under these Regulations or another law; and

(ii) can be disclosed without disclosing, expressly or by implication, other information to which subregulation (3) or (4) applies.

(6) Subregulations (3) and (4) do not limit the authority of an Agency Head to give lawful and reasonable directions in relation to the disclosure of information.

Note Under section 70 of the *Crimes Act 1914*, it is an offence for an APS employee to publish or communicate any fact or document which comes to the employee's knowledge, or into the employee's possession, by virtue of being a Commonwealth officer, and which it is the employee's duty not to disclose.