



**Australian Government**

---

**ENHANCING NATIONAL PRIVACY  
PROTECTION**

**Australian Government  
First Stage Response**

to the

**Australian Law Reform Commission Report 108**

***For Your Information: Australian Privacy Law and Practice***

**October 2009**

---

**Cabinet Secretary, Senator the Hon Joe Ludwig**





**Australian Government**

**Australian Government  
First Stage Response**

**to the**

**Australian Law Reform Commission Report 108**

***For Your Information: Australian Privacy Law and Practice***

**October 2009**



## Message from the Cabinet Secretary



I am pleased to announce the Australian Government's first stage of reforms to enhance the protection of personal privacy, responding to the Australian Law Reform Commission's inquiry into the effectiveness of the *Privacy Act 1988*.

In 21<sup>st</sup> century Australia, the dissemination of our personal information is pervasive. Our society is moving further and further away from our traditional means of communicating, yet most Australians don't consider one of our main means of electronically sharing of information - the internet - to be a secure way of providing information.

This push toward greater electronic sharing of information is often desirable, but when it isn't it may be hard to avoid. We are encouraged to create paperless workplaces; we conduct business in a global economy, and in doing so we unknowingly give our information to customer service providers overseas; we log into social networking sites and blog daily, accessing the internet and emails at the click of a button on our mobile phones.

While our personal information is becoming more difficult to control, people are becoming more aware of their right to privacy. However, Australia's laws haven't kept up with the considerable changes in our society that have occurred since the *Privacy Act 1988* was enacted over 20 years ago.

The Rudd Government recognises that we now need a robust and adaptable privacy framework which protects our privacy while also allowing for future technological developments and other improvements that will increase efficiencies in our economy and ensure the safety of our society.

Such a framework must meet community expectations of fairness, transparency, security and individual participation in the handling of personal information. It must also complement government and business activities and allow appropriate flows of personal information that individuals and the community expect, such as information sharing that is necessary to enforce the law and prevent crime.

The Australian Government is responding to these challenges by embarking on the most significant reforms of privacy law since the *Privacy Act's* inception.

These reforms respond to 197 of the Australian Law Reform Commission's 295 recommendations for improving privacy protection, which were made in its report: *For Your Information: Australian Privacy Law and Practice*. When the report was released in August 2008, the Australian Government committed to responding in two stages.

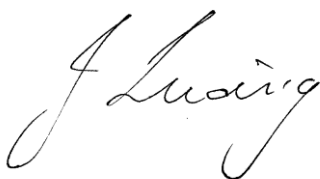
This, the Government's first stage response, focuses on establishing the foundations. The Government will outline a clear and simple framework for privacy rights and obligations and build on its commitment to trust and integrity in Government. The Government will:

- create a harmonised set of Privacy Principles which will replace the separate sets of public and private sector principles at the federal level, untangling red tape and marking a significant step on the road to national consistency;
- redraft and update the Privacy Act to make the law clearer and easier to comply with;
- create a comprehensive credit reporting framework which will improve individual credit assessments, complimenting the Government's reforms to responsible lending practices;
- improve health sector information flows, and give individuals new rights to control their health records, contributing to better health service delivery;
- require the public and private sector to ensure the right to privacy will continue to be protected if personal information is sent overseas; and
- strengthen the Privacy Commissioner's powers to conduct investigations, resolve complaints and promote compliance, contributing to more effective and stronger protection of the right to privacy.

These reforms will be technology neutral, providing protection for personal information held in any medium. The Privacy Commissioner will also have an enhanced role in researching, guiding and educating on technologies that enhance or impact on privacy. Even as we find newer and faster ways to interconnect, individuals are unlikely to abandon the right to privacy, or the desire to choose where their information goes. The Government will ensure that the right to privacy is protected well in to the future.

We will start with reforming the foundations. Once these reforms have progressed, the Government will turn to considering the remaining recommendations of the ALRC. These recommendations include sensitive and complex questions around the removal of exemptions and data breach notices. To strike the right balance, reforms in these areas will require extensive consultation and input.

In announcing these reforms, I must acknowledge the significant investment and contribution that stakeholders made to develop these reforms. Thank you to the Australian Law Reform Commission, the Department of the Prime Minister and Cabinet, and all of the stakeholders who contributed their valuable time, energy and experience to this important law reform process. I look forward to your further input on the first stage of reform when I release exposure draft legislation for consultation, and to starting a dialogue on the 'second stage' recommendations in the future.



JOE LUDWIG  
Cabinet Secretary and Special Minister of State

# Table of Contents

<b>MESSAGE FROM THE CABINET SECRETARY .....</b>	<b>5</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>9</b>
<b>SUMMARY TABLE OF GOVERNMENT RESPONSE TO RECOMMENDATIONS ADDRESSED IN THE FIRST STAGE 15</b>	
<b>GOVERNMENT RESPONSE TO RECOMMENDATIONS.....</b>	<b>21</b>
PART A – INTRODUCTION (PRIVACY ACT: STRUCTURE, OBJECTS, DEFINITIONS AND SCOPE) .....	21
3. <i>Achieving National Consistency</i> .....	21
5. <i>The Privacy Act: Name, Structure and Objects</i> .....	22
6. <i>The Privacy Act: Some Important Definitions</i> .....	24
7. <i>Privacy Beyond the Individual</i> .....	27
8. <i>Privacy of Deceased Individuals</i> .....	28
PART B – DEVELOPING TECHNOLOGY .....	30
10. <i>Accommodating Developing Technology in a Regulatory Framework</i> .....	30
11. <i>Individuals, the Internet and Generally Available Publications</i> .....	32
PART C – INTERACTION, INCONSISTENCY AND FRAGMENTATION .....	33
15. <i>Federal Information Laws</i> .....	33
16. <i>Required or Authorised by or Under Law</i> .....	34
PART D – THE PRIVACY PRINCIPLES.....	37
18. <i>Structural Reform of the Privacy Principles</i> .....	37
19. <i>Consent</i> .....	38
20. <i>Anonymity and Pseudonymity</i> .....	39
21. <i>Collection</i> .....	40
22. <i>Sensitive Information</i> .....	43
23. <i>Notification</i> .....	45
24. <i>Openness</i> .....	48
25. <i>Use and Disclosure</i> .....	52
26. <i>Direct Marketing</i> .....	56
27. <i>Data Quality</i> .....	61
28. <i>Data Security</i> .....	62
29. <i>Access and Correction</i> .....	64
30. <i>Identifiers</i> .....	73
31. <i>Cross-border Data Flows</i> .....	77
44. <i>New Exemptions or Exceptions (Confidential Alternative Dispute Resolution Processes)</i> .....	82
PART F – OFFICE OF THE PRIVACY COMMISSIONER .....	83
46. <i>Structure of the Office of the Privacy Commissioner</i> .....	83
47. <i>Powers of the Office of the Privacy Commissioner</i> .....	85
48. <i>Privacy Codes</i> .....	89
49. <i>Investigation and Resolution of Privacy Complaints</i> .....	91
50. <i>Enforcing the Privacy Act</i> .....	97
PART G – CREDIT REPORTING PROVISIONS.....	99
54. <i>Approach to Reform</i> .....	99
55. <i>More Comprehensive Credit Reporting</i> .....	105
56. <i>Collection and Permitted Content of Credit Reporting Information</i> .....	109
57. <i>Use and Disclosure of Credit Reporting Information</i> .....	115
58. <i>Data Quality and Security</i> .....	120
59. <i>Access and Correction, Complaint Handling and Penalties</i> .....	124
PART H – HEALTH SERVICES AND RESEARCH .....	129
60. <i>Regulatory Framework for Health Information</i> .....	129
61. <i>Electronic Health Information Systems</i> .....	131
62. <i>The Privacy Act and Health Information</i> .....	132
63. <i>Privacy (Health Information) Regulations (Health-specific reforms to the Privacy Principles)</i> .....	133
65. <i>Research: Recommendations for Reform</i> .....	139
66. <i>Research: Databases and Data Linkage</i> .....	144





## Executive Summary

This is the first stage of the Australian Government's response to the Australian Law Reform Commission's Report 108, *For Your Information: Australian Privacy Law and Practice* ('the ALRC report').

The ALRC report was the product of a comprehensive 28 month inquiry into the effectiveness of the *Privacy Act 1988* ('Privacy Act') and related laws. Released on 11 August 2008, the report involved an extensive research process and the largest community consultation program in the ALRC's history.<sup>1</sup>

The overwhelming message from the ALRC's consultations was that 'Australians do care about privacy, and they want a simple, workable system that provides effective solutions and protections.'<sup>2</sup> The ALRC found that 'the Privacy Act has worked well to date, but that it now needs a number of refinements to bring it up to date with the information age.'<sup>3</sup> At the same time, the consultations found that there continues to be strong concerns about complexity of the law and confusion around the application of overlapping privacy laws at the federal, state and territory levels.<sup>4</sup>

The Government's first stage response is informed by the ALRC's findings and further consultation which was undertaken by the Department of the Prime Minister and Cabinet. The Department's additional consultations began in October 2008 and included:

- stakeholder roundtables in Canberra, Melbourne and Sydney;
- public submissions; and
- bilateral consultations with agencies, industry and consumer representatives, academics and privacy experts.

The first stage response addresses 197 of the 295 recommendations in the ALRC's report. Of those 197 recommendations:

- the Government has accepted 141, either in full or in principle;
- 34 are accepted with qualification;
- 20 are not accepted; and
- 2 recommendations are noted.

Many of these require legislative amendment to the Privacy Act.

The focus of the first stage response is to establish the foundations for an enhanced privacy framework. The remaining 98 recommendations of the ALRC will be considered in stage two of the Government's response (see below).

---

<sup>1</sup> ALRC, Report 108, Executive Summary, 'Extensive public engagement'.

<sup>2</sup> ALRC, Report 108, Outline of the Report: <http://www.alrc.gov.au/inquiries/title/alrc108/outline.html>.

<sup>3</sup> Ibid.

<sup>4</sup> ALRC, Report 108, Executive Summary, 'Complexity and confusion'.

## **Structure of the first stage response**

The Government's first stage response follows the structure of the relevant Parts of the ALRC report, although some titles have changed to better reflect the response.

- **Part A – The Privacy Act: Name, Structure, Objects, Definitions and Scope**
- **Part B – Developing Technology**
- **Part C – Interaction, Inconsistency and Fragmentation**
- **Part D – The Privacy Principles**
- **Part F – Office of the Privacy Commissioner: Powers and Functions**
- **Part G – Credit Reporting Provisions**
- **Part H – Health Services and Research**

Each section of this response sets out the relevant ALRC recommendation, whether the Government accepts it, and any further comments on the Government's position.

### **Part A – The Privacy Act: Name, Structure, Objects, Definitions, and Scope**

These recommendations primarily relate to introductory issues which underpin a new privacy framework. The Government will redraft the Privacy Act to improve its structure, ensure clarity and consistency. The redrafted Act will include an objects clause to guide interpretation and the exercise of relevant powers and functions. Definitions will also be clarified and brought up-to-date.

### **Part B – Developing Technology**

These recommendations relate to the interaction between new technologies and privacy, respond to the impact of digital media, to the increasing ability to store and transfer personal information, and to other developments in technology that have occurred since the Privacy Act was enacted over 20 years ago.

The Government's response supports a renewed role for the Privacy Commissioner to conduct research, and to guide and educate Australians on technologies that impact on or enhance privacy. The Privacy Act will be technology neutral and recommendations in other parts of the response will further protect Australians against emerging threats and privacy pitfalls. These include:

- provisions for sector-developed privacy codes, and discretion for the Privacy Commissioner to require codes to be developed where appropriate;
- the Commissioner's ability to establish ad hoc expert advisory panels; and
- the inclusion of biometric information in the definition of 'sensitive information' (reflecting its unique nature and heightened risks of misuse).

## **Part C – Interaction, Inconsistency and Fragmentation**

Part C of the ALRC's report considers the interaction between the Privacy Act and other federal, state and territory laws. The impact of other laws on the protection of privacy will be considered by the Government and reflected both within the Privacy Act and in other legislation. The Government will continue to consider the impact of other laws on the protection of privacy on an ongoing basis.

## **Part D – The Privacy Principles**

Underpinning the enhanced protection of privacy is a simple and clear framework. This part of the ALRC's report makes recommendations for a single set of Privacy Principles.

The Government will enact a single set of Privacy Principles to protect personal information held by both Australian Government agencies (agencies) and relevant businesses in the private sector (organisations). These streamlined Privacy Principles (which the ALRC referred to in its report as Uniform Privacy Principles (UPPs)) will replace the existing Information Privacy Principles and National Privacy Principles that currently exist.

The Government agrees with the ALRC that principles-based law remains the best regulatory model for the protection of an individual's privacy in Australia. High-level principles provide baseline protections for personal information held in any form, while giving agencies and organisations the flexibility to tailor information handling practices to their diverse needs. The Privacy Commissioner will continue to play an integral role in guiding agencies, organisations and individuals on the application of the Privacy Principles and the Privacy Act, in addition to oversight and enforcement roles.

The single set of binding Privacy Principles will be structured to better reflect the stages of the information handling process. The Privacy Principles will deal with core aspects of privacy including openness (privacy policies and practices), options for anonymity and pseudonymity, collection, notification, use and disclosure, data quality and security, and access to and correction of personal information.

The Principles will also outline specific requirements for matters such as use and disclosure for the purposes of direct marketing, handling of government identifiers, cross-border data flows (overseas transfer), health and credit reporting information.

New Government proposals for the Privacy Principles include:

- a requirement to take reasonable steps to implement compliance with the Privacy Principles, under the 'openness' principle;
- a 'missing persons' exception under the 'use and disclosure' principle;
- greater accountability for entities that transfer information overseas under the 'cross-border data flows' principle; and
- specific permission to handle Commonwealth, state and territory government identifiers for identity verification purposes under the 'identifiers' principle.

*Note:* The ALRC's report provided a proposed model for its recommended UPPs. However, the Government is responding to the policy intent of individual recommendations, and is not responding directly to the form or drafting of the model UPPs. The Government will determine the most appropriate way to give effect to the policy intent when it drafts the necessary amendments to the Privacy Act.

## **Part F – Office of the Privacy Commissioner**

In its report, the ALRC made a number of recommendations relating to the structure, powers, and functions of the Privacy Commissioner. The Government response sets out a range of additional functions and powers that the Privacy Commissioner will have to investigate and resolve complaints and to promote and enforce compliance. This will include discretionary powers to:

- require agencies to conduct 'privacy impact assessments' where appropriate;
- undertake 'privacy performance assessments' of organisations' activities;
- handle complaints and gather information more effectively, compel appearances or production of documents, and accept enforceable undertakings; and
- seek civil penalties for serious or repeated breaches of the Privacy Act.

*Note:* The Privacy Commissioner's role as part of a new Office of the Information Commissioner is explained further below.

## **Part G – Credit Reporting Provisions**

The Government accepts the ALRC's recommendations to introduce comprehensive credit reporting in Australia, which will be supported by the protections in the Privacy Principles along with more specific and different provisions directly related to credit reporting. The Government will introduce five positive datasets into the credit reporting system.<sup>5</sup> This will benefit business and consumers through improved assessment of individual credit worthiness and increased competition between large and small lenders.

To address privacy and consumer concerns around comprehensive credit reporting, repayment history information will not be available until new responsible lending obligations are in place. These new obligations are proposed under the National Consumer Credit Protection Bill 2009.

The Government's response also outlines measures to make the credit regime more flexible and less prescriptive, including:

- requiring the industry to develop a mandatory and binding credit reporting code, with detailed standards for consistent compliance;
- emphasising industry-led complaint resolution through external dispute resolution and greater responsibility on credit providers and credit reporting agencies;
- prohibiting direct marketing using credit information, but permitting pre-screening of direct marketing lists to remove adverse credit risks (with provision to opt-out); and
- reforms to enhance consumer protection and awareness of adverse listings.

---

<sup>5</sup> The five new datasets are: the type of each active credit account, date of opening *and* closure of account, account credit limits and credit repayment history (recommendations 55-1 and 55-2 refer).

## **Part H – Health Services and Research**

The ALRC made a number of recommendations to clarify definitions and address a range of health privacy issues, while retaining core provisions in line with confidentiality obligations and professional ethics. The Government will amend the Privacy Principles to:

- enact new rights for individuals to have their health records transferred between health service providers (reasonable fees may apply), and to be told what will happen to their health record if their provider closes down or changes hands;
- clarify that providers can share health information that is necessary for healthcare and is within the individual's reasonable expectations, promoting appropriate information flows in the sector; and
- strengthen options for access through an 'intermediary', with a tailored option if direct access to health information seriously threatens life, health or safety.

The Government will also work with other jurisdictions and health ministers to progress national consistency in the public and private health sectors.

The Government's response also supports two central proposals to facilitate research in the public interest, simplify regulation, and protect community expectations of personal privacy:

- a harmonised set of rules for Government and private sector researchers will replace the two sets of binding guidelines on non-consensual handling of personal information; and
- the research provisions will be expanded to allow such handling for any research in the public interest, not just for health and medical research.

Two important parameters of the current regime will also be maintained:

- the public interest in research must 'substantially outweigh' the protection of privacy – requiring a clear choice in favour of the research; and
- the National Health & Medical Research Council and the Privacy Commissioner will retain primary responsibility for issuing and approving the research rules.

### **Towards national consistency**

The transition to a single set of Privacy Principles will mark a significant step toward consistent privacy laws in Australia. For the first time, a single privacy regime will apply across the private sector and to the Commonwealth public sector.

In giving its first stage response, the Government will create a platform from which it can pursue national harmonisation through discussion with the states and territories.

Ultimately, the aim will be a consistent set of privacy standards for the Commonwealth, state and territory public sectors, as well as the private sector.

Additional national consistency issues will be considered in the Government's second stage response.

## **Next steps for implementation**

With the release of its first stage response to the ALRC report, the Government will begin preparing exposure draft legislation to implement the proposed changes. The exposure draft will be released in early 2010 for further consultation.

The second stage of the Government's response will consider the remaining 98 recommendations of the ALRC. These recommendations include issues such as:

- proposals to clarify or remove certain exemptions from the Privacy Act (such as the exemptions for small businesses and employee records);
- introducing a statutory cause of action for serious invasion of privacy (beyond 'personal information');
- serious data breach notifications;
- privacy and decision making issues for children and authorised representatives; and
- handling of personal information under the *Telecommunications Act 1997*.

Due to the complexity and sensitivity of the remaining recommendations, the Government will consult extensively with the public and private sectors before responding to the stage two recommendations. This consultation will be undertaken once the first stage of the response has been progressed.

## **Relationship to the Office of the Information Commissioner reforms**

As part of its 2007 election policy, *Government Information: restoring trust and integrity*, the Government committed to bringing the function of privacy protection within a new Office of the Information Commissioner (OIC) which would be responsible for both privacy and freedom of information (FOI) laws.

In March 2009, the Government released exposure draft legislation to implement this commitment. Under the proposed reforms, the Privacy Commissioner will be one of three independent statutory office-holders in the new agency. The Privacy Commissioner and an FOI Commissioner will operate under the leadership of an Information Commissioner as the agency's CEO.

While formal powers will be vested in the Information Commissioner, the Privacy Commissioner will continue to have a role in exercising relevant powers and functions. For consistency with the ALRC report's recommendations, this response continues to refer to the Privacy Commissioner and the Office of the Privacy Commissioner rather than the Office of the Information Commissioner.

## Summary table of Government response to recommendations addressed in the first stage

This table summarises the Government's response to the recommendations from the ALRC report that are being addressed in the first stage of its response.

Of the 197 recommendations that are addressed in the first stage:

- 175 have been accepted, accepted in principle, accepted in part, or accepted with amendment;
- 20 have not been accepted; and
- 2 have been noted.

The remaining 98 recommendations made by the ALRC will be addressed in the second stage of the Government's response.

References in this table to Parts, Chapters and Recommendation numbers generally reflect references used in the ALRC report.

Part reference	Chapter reference	Rec	Response
<b>Introduction</b> (Part A)  <i>(Privacy Act: Structure, Objects, Definitions &amp; Scope)</i>	Achieving National Consistency	3-1	Accept in principle
		3-2	Accept in principle
	The Privacy Act: Name, Structure and Objects	5-1	Not accept
		5-2	Accept
		5-3	Not accept
		5-4	Accept in principle
	The Privacy Act: Some Important Definitions	6-1	Accept
		6-2	Accept
		6-3	Accept
		6-4	Accept
		6-5	Accept
		6-6	Accept
		6-7	Accept
	Privacy Beyond the Individual	7-1	Accept
		7-2	Not accept
	Privacy of Deceased Individuals	8-1	Not accept
		8-2	Not accept
		8-3	Not accept
<b>Developing Technology</b> (Part B)	Accommodating Developing Technology in a Regulatory Framework	10-1	Accept
		10-2	Accept
		10-3	Accept in principle
		10-4	Accept
	Individuals, the Internet and Generally Available Publications	11-1	Accept
		11-2	Not accept
<b>Interaction, Inconsistency and</b>	Federal Information Laws	15-1	Not accept
		15-2	Accept
		15-3	Noted

<b>Fragmentation</b> (Part C)	Required or Authorised by or Under Law	16-1	Accept in principle
		16-2	Accept
		16-3	Accept
		16-4	Accept in principle
<b>Unified Privacy Principles</b> (Part D)	Structural Reform of the Privacy Principles	18-1	Accept
		18-2	Accept
	Consent	19-1	Accept with amendment
	Anonymity and Pseudonymity	20-1	Accept
		20-2	Accept
	Collection	21-1	Accept
		21-2	Accept
		21-3	Accept
		21-4	Accept
		21-5	Accept
	Sensitive Information	22-1	Accept
		22-2	Accept
		22-3	Accept in part
	Notification	23-1	Accept
		23-2	Accept with amendment
		23-3	Accept
	Openness	24-1	Accept with amendment
		24-2	Accept
		24-3	Accept
	Use and Disclosure	25-1	Accept
		25-2	Accept with amendment
		25-3	Accept with amendment
	Direct Marketing	26-1	Accept with amendment
		26-2	Accept
		26-3	Accept with amendment
		26-4	Accept in part
		26-5	Accept with amendment
		26-6	Accept with amendment
		26-7	Accept
	Data Quality	27-1	Accept
	Data Security	28-1	Accept
		28-2	Noted
		28-3	Accept
		28-4	Accept
		28-5	Accept
	Access and Correction	29-1	Accept
		29-2	Accept
		29-3	Accept with amendment
		29-4	Accept
		29-5	Accept
		29-6	Accept in principle
		29-7	Accept with amendment
		29-8	Accept with amendment
		29-9	Accept
	Identifiers	30-1	Accept
		30-2	Accept in principle
		30-3	Not accept



		30-4	Accept in principle
		30-5	Accept in principle
		30-6	Accept in principle
		30-7	Accept
	Cross-border Data Flows	31-1	Accept
		31-2	Accept with amendment
		31-3	Accept
		31-4	Accept
		31-5	Accept
		31-6	Accept
		31-7	Accept
		31-8	Accept
	New Exemptions or Exceptions (Confidential ADR processes) <sup>6</sup>	44-1	Accept
44-2		Accept	
<b>Office of the Privacy Commissioner</b> (Part F)  <i>(Structure and Powers of the Privacy Commissioner)</i>	Structure of the Office of the Privacy Commissioner	46-1	Not accept
		46-2	Not accept
		46-3	Accept
		46-4	Accept with amendment
		46-5	Accept
	Powers of the Office of the Privacy Commissioner	47-1	Accept
		47-2	Accept
		47-3	Accept
		47-4	Accept
		47-5	Accept
		47-6	Accept
		47-7	Accept
		47-8	Accept in principle
	Privacy Codes	48-1	Accept in principle
	Investigation and Resolution of Privacy Complaints	49-1	Accept
		49-2	Accept
		49-3	Not accept
		49-4	Accept
		49-5	Accept with amendment
		49-6	Accept in principle
		49-7	Accept in principle
		49-8	Accept
		49-9	Accept
		49-10	Accept
		49-11	Accept
		49-12	Accept
		49-13	Accept
	Enforcing the Privacy Act	50-1	Accept
		50-2	Accept in principle
		50-3	Accept
		50-4	Accept
<b>Credit Reporting</b> (Part G)	Approach to Reform	54-1	Not accept
		54-2	Accept
		54-3	Accept
		54-4	Accept

<sup>6</sup> This recommendation was in Part E –Exemptions of the ALRC’s report.

		54-5	Accept
		54-6	Accept in principle
		54-7	Not accept
		54-8	Accept in principle
		54-9	Accept with amendment
	More Comprehensive Credit Reporting	55-1	Accept
		55-2	Accept
		55-3	Accept
		55-4	Accept in principle
		55-5	Accept
	Collection and Permitted Content of Credit Reporting Information	56-1	Accept
		56-2	Accept
		56-3	Accept
		56-4	Accept in principle
		56-5	Accept
		56-6	Accept
		56-7	Accept in principle
		56-8	Accept
		56-9	Accept
		56-10	Accept
		56-11	Accept with amendment
	Use and Disclosure of Credit Reporting Information	57-1	Accept
		57-2	Not accept
		57-3	Accept in part
		57-4	Accept in principle
		57-5	Accept
		57-6	Not accept
	Data Quality and Security	58-1	Accept
		58-2	Accept
		58-3	Accept
		58-4	Accept
		58-5	Accept
		58-6	Accept with amendment
	Access and Correction, Complaint Handling and Penalties	59-1	Accept
		59-2	Accept in principle
		59-3	Accept
		59-4	Accept
		59-5	Accept in part
		59-6	Accept
		59-7	Accept with amendment
		59-8	Accept
		59-9	Accept
<b>Health Services and Research (Part H)</b>	Regulatory Framework for Health Information	60-1	Not accept
		60-2	Not accept
		60-3	Accept in principle
	Electronic Health Information Systems	61-1	Accept in principle
	Health Information	62-1	Accept
		62-2	Accept with amendment
	Overall Reform for Health Privacy	63-1	Accept
		63-2	Accept

		63-3	Accept with amendment
		63-4	Not accept
		63-5	Accept with amendment
		63-6	Accept with amendment
		63-7	Accept with amendment
		63-8	Accept
		63-9	Accept with amendment
		63-10	Not accept
	Research: Recommendations for Reform	65-1	Accept with amendment
		65-2	Accept
		65-3	Accept
		65-4	Accept with amendment
		65-5	Accept in part
		65-6	Accept
		65-7	Accept
		65-8	Accept with amendment
		65-9	Accept with amendment
	Research: Databases and Data Linkage	66-1	Accept in principle
		66-2	Accept in principle
		66-3	Accept in principle



## Government response to recommendations

### PART A – INTRODUCTION

#### (Privacy Act: Structure, Objects, Definitions and Scope)

### 3. Achieving National Consistency

**Recommendation 3–1** The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

- (a) *Health Records and Information Privacy Act 2002* (NSW);
- (b) *Health Records Act 2001* (Vic);
- (c) *Health Records (Privacy and Access) Act 1997* (ACT); and
- (d) any other laws prescribed in the regulations.

#### **Response: Accept in principle**

The Government recognises there are clear benefits of nationally consistent privacy regulation in the private sector, including the health sector. The Government will work with its state and territory counterparts to progress this matter through further discussions in appropriate fora.

**Recommendation 3–2** States and territories with information privacy legislation that purports to apply to organisations should amend that legislation so that it no longer applies to organisations.

#### **Response: Accept in principle**

This is a matter for state and territory governments and will be the subject of further discussions with those governments at the appropriate time.

## 5. The Privacy Act: Name, Structure and Objects

**Recommendation 5–1** The regulation-making power in the Privacy Act should be amended to provide that the Governor-General may make regulations, consistent with the Act, modifying the operation of the model Unified Privacy Principles (UPPs) to impose different or more specific requirements, including imposing more or less stringent requirements, on agencies and organisations than are provided for in the UPPs.

### **Response: Not accept**

The Government considers modification of the Privacy Principles should, wherever possible, be contained in the Privacy Act to ensure that Parliament has an express role in determining whether changes are made to fundamental privacy protections. This will ensure that any significant changes to the application of the Privacy Principles are in the primary legislation. This approach will reduce any complexity and confusion that could result from having multi-layered regulation of privacy as proposed by the ALRC.

Changes to the operation of the Privacy Principles will only be made in clearly defined circumstances by specific regulation, but otherwise will be modified within the Privacy Act itself. The Privacy Commissioner will continue to be able to modify the application of the Privacy Principles in discrete circumstances by making a public interest determination (PID). The PID process provides sufficient flexibility for the Privacy Act to accommodate changing circumstances, as necessary. However any significant modifications to the Privacy Principles should occur within primary legislation.

**Recommendation 5–2** The *Privacy Act* should be redrafted to achieve greater logical consistency, simplicity and clarity.

### **Response: Accept**

Given the number of amendments which are intended to be made to the Privacy Act in response to the ALRC recommendations, some elements of the Act will require extensive re-drafting (most notably the consolidation of the Information Privacy Principles and the National Privacy Principles into the Privacy Principles). These amendments will provide an opportunity to redraft the Privacy Act to make it more user-friendly for individuals, organisations and agencies.

**Recommendation 5–3** The *Privacy Act* should be renamed the *Privacy and Personal Information Act*. If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, however, the name of the Act should remain the same.

### **Response: Not accept**

The Government does not consider that it is necessary to rename the Privacy Act. The Government believes that the public is generally aware of the scope and application of the Act. The current name has been in place for over 20 years, provides a clear and simple message about the Act's objectives and sufficiently differentiates the Act from the legislation

in other jurisdictions.

The Government also notes that it is responding to the ALRC's report in two stages, with consideration of the statutory cause of action for invasion of privacy deferred until the second stage. It would be inappropriate to change the name of the Act prior to considering this recommendation.

**Recommendation 5–4** The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be specified to:

- (a) implement, in part, Australia's obligations at international law in relation to privacy;
- (b) recognise that individuals have a right to privacy and to promote the protection of that right;
- (c) recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests;
- (d) provide the basis for nationally consistent regulation of privacy and the handling of personal information;
- (e) promote the responsible and transparent handling of personal information by agencies and organisations;
- (f) facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy;
- (g) establish the Australian Privacy Commission and the position of the Privacy Commissioner; and
- (h) provide an avenue for individuals to seek redress when there has been an alleged interference with their privacy.

**Response: Accept in principle**

The Government acknowledges that it is desirable to have an objects clause which clearly outlines the underlying purpose of the Privacy Act in order to assist in its interpretation. The Government notes that the proposed objects clause as recommended by the ALRC is based broadly on the current application of the Privacy Act along with changes proposed by the ALRC.

While the Government broadly supports the proposed objects, the objects clause will be drafted to reflect the Government's position on the recommendations in this first stage response. For example, paragraph (g) may need to be revised to reflect the Government's establishment of the Office of the Information Commissioner.

## 6. The Privacy Act: Some Important Definitions

**Recommendation 6–1** 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’.

### **Response: Accept**

The Government agrees it is important for the definition of personal information to be sufficiently flexible and technology-neutral to encompass changes in the way that information that identifies an individual is collected and handled. The ALRC’s recommended definition continues to allow this approach and also brings the definition in line with international standards and precedents.

The proposed definition does not significantly change the scope of what is considered to be personal information. The application of ‘reasonably identifiable’ ensures the definition continues to be based on factors which are relevant to the context and circumstances in which the information is collected and held. The Government proposes that this element of the definition will be informed by whether it would be reasonable and practicable to identify the individual from both the information itself and other reasonably accessible information.

**Recommendation 6–2** The Office of the Privacy Commissioner should develop and publish guidance on the meaning of ‘identified or reasonably identifiable’.

### **Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

The Government agrees that guidance issued by the Office of the Privacy Commissioner would play an important role in assisting organisations, agencies and individuals to understand the application of the new definition, especially given the contextual nature of the definition.



**Recommendation 6–3** The Office of the Privacy Commissioner should develop and publish guidance on the meaning of ‘not reasonably identifiable’.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

The Government notes that this recommendation is directly related to any guidance issued in relation to recommendation 6-2 and recommendation 28-5 (that the Office of the Privacy Commissioner should develop and publish guidance on the manner in which information is rendered non-identifiable for the purpose of the ‘data security’ principle). Guidance would allow for a more flexible and nuanced approach to determining when personal information is ‘de-identified’ and does not make the individual ‘reasonably identifiable’.

**Recommendation 6–4** The definition of ‘sensitive information’ in the *Privacy Act* should be amended to include:

- (a) biometric information collected for the purpose of automated biometric verification or identification; and
- (b) biometric template information.

**Response: Accept**

The Government recognises the importance of attributing a higher level of protection to personal information which is sensitive in nature. The Government agrees that biometric information has similar attributes to other sensitive information and it is desirable to provide it with a higher level of protection.

Given the broad nature of what can be considered biometric information, the definition should make clear that the additional protections should only extend to that biometric information which is specifically being collected to identify or verify an individual through biometric processes.

**Recommendation 6–5** The definition of ‘sensitive information’ in the *Privacy Act* should be amended to refer to ‘sexual orientation and practices’ rather than ‘sexual preferences and practices’.

**Response: Accept**

The Government notes that this is a minor change which is not intended to change the meaning of the definition but will ensure consistency with other Commonwealth, state and territory legislation.

**Recommendation 6–6** The definition of ‘record’ in the *Privacy Act* should be amended to make clear that a record includes:

- (a) a document (as defined in the *Acts Interpretation Act 1901* (Cth)); and
- (b) information stored in electronic or other format.

**Response: Accept**

The Government notes that the ALRC’s recommendation is not intended to expand the scope of the current definition of record. The recommendation aims to streamline the definition to ensure that it is consistent with its use in similar legislation.

The Government agrees that the definition should be inclusive and encompass a broad range of recorded information, including information held in electronic format. This will ensure that the definition is sufficiently flexible to encompass how information will be recorded and stored in the future.

**Recommendation 6–7** The definition of ‘generally available publication’ in the *Privacy Act* should be amended to clarify that a publication is ‘generally available’ whether or not a fee is charged for access to the publication.

**Response: Accept**

The Government agrees that this amendment will clarify the application of the definition of ‘generally available publication’.

## 7. Privacy Beyond the Individual

**Recommendation 7–1** The Office of the Privacy Commissioner should encourage and assist agencies and organisations to develop and publish protocols, in consultation with Indigenous groups and representatives, to address the particular privacy needs of Indigenous groups.

**Response: Accept**

The Government acknowledges the important role the Office of the Privacy Commissioner plays in assisting agencies and organisations to develop appropriate mechanisms to protect privacy. The Government encourages the Office to provide assistance to develop protocols for Indigenous groups where appropriate and necessary and in consultation with appropriate Indigenous bodies.

**Recommendation 7–2** The Australian Government should undertake an inquiry to consider whether legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take.

**Response: Not accept**

This recommendation is outside the ALRC's Terms of Reference for the report.

The Government notes that both Commonwealth intellectual property and cultural heritage legislation provide protections for Aboriginal and Torres Strait Islander peoples' cultural rights. Government agencies are working closely together to develop approaches to address the complex issues around protecting cultural rights at both the domestic and international level.

## 8. Privacy of Deceased Individuals

**Recommendation 8–1** The *Privacy Act* should be amended to include provisions dealing with the personal information of individuals who have been dead for 30 years or less where the information is held by an organisation. The Act should provide as follows:

(a) Use and Disclosure

Organisations should be required to comply with the ‘Use and Disclosure’ principle in relation to the personal information of deceased individuals. Where the principle would have required consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. The organisation must not use or disclose the information if the use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

(b) Access

Organisations should be required to provide third parties with access to the personal information of deceased individuals in accordance with the access elements of the ‘Access and Correction’ principle, except to the extent that providing access would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

(c) Data Quality

Organisations should be required to comply with the use and disclosure elements of the ‘Data Quality’ principle in relation to the personal information of deceased individuals.

(d) Data Security

Organisations should be required to comply with the ‘Data Security’ principle in relation to the personal information of deceased individuals.

### **Response: Not accept**

The Government acknowledges that there are arguments both for and against extending privacy protections to personal information about deceased persons where held by organisations. Having taken further advice on this issue, the Government is aware of the significant constitutional limitations on the Commonwealth’s power to legislate in this area. The Government therefore does not accept the ALRC’s recommendations 8-1 to 8-3.

The Privacy Act will continue to apply to living persons only (with the exception of Part VIA on declared emergencies). Existing sectoral laws and professional duties will continue to apply to personal information about deceased persons. This includes obligations of confidentiality, testamentary and estates law, records retention regulations and other relevant Commonwealth, state and territory laws.

The *Freedom of Information Act 1982* and the *Archives Act 1983* will continue to apply to information about deceased persons that is held by Australian Government agencies.

The Government encourages the Office of the Privacy Commissioner to provide ongoing education regarding the fact that the Privacy Act does not apply to information about deceased persons, and any other guidance on this issue that the Privacy Commissioner deems appropriate.

**Recommendation 8–2** The *Privacy Act* should be amended to provide that the content of National Privacy Principle 2.1(ea) on the use and disclosure of genetic information to genetic relatives—to be moved to the new *Privacy (Health Information) Regulations* in accordance with Recommendation 63–5—should apply to the use and disclosure of genetic information of deceased individuals.

**Response: Not accept**

As outlined in response to recommendation 8-1, the Privacy Act will continue to apply to personal information about living persons only.

**Recommendation 8–3** Breach of the provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner:

- (a) in relation to an alleged breach of the use and disclosure, access, data quality or data security provisions—the deceased individual’s parent, child or sibling who is aged 18 or over, spouse, de facto partner or legal personal representative; and
- (b) in relation to an alleged breach of the access provision—the parties in paragraph (a) and any person who has made a request for access to the personal information of a deceased individual where that request has been denied.

**Response: Not accept**

As outlined in response to recommendation 8-1, the Privacy Act will continue to apply to personal information about living persons only.

## PART B – DEVELOPING TECHNOLOGY

### 10. Accommodating Developing Technology in a Regulatory Framework

**Recommendation 10–1** In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations.

**Response: Accept**

The Government encourages the Privacy Commissioner to exercise his or her discretion in conducting research on matters relating to privacy, including privacy enhancing technologies.

It would assist in promoting good privacy practice for such research to be made publicly available where appropriate.

**Recommendation 10–2** The Office of the Privacy Commissioner should develop and publish educational materials for individuals, agencies and organisations about specific privacy-enhancing technologies and the privacy-enhancing ways in which technologies can be deployed.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

Such materials should be developed in consultation with relevant government bodies (including of the states and territories), consumer and industry stakeholders.

To ensure consistency in approaches to guidance materials, agencies with functions relating to privacy and new technologies should consider cooperative approaches to the development and publication of relevant educational materials.

**Recommendation 10–3** The Office of the Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy. This guidance should incorporate relevant local and international standards. Matters that such guidance should address include:

- (a) developing technologies such as radio frequency identification (RFID) or data-collecting software such as ‘cookies’;
- (b) when the use of a certain technology to collect personal information is not done by ‘fair means’ and is done ‘in an unreasonably intrusive way’;
- (c) when the use of a certain technology will require agencies and organisations to notify individuals at or before the time of collection of personal information;
- (d) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometric systems);
- (e) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information in an intelligible form (for example, the type of biometric information that is held as a biometric template); and
- (f) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.

**Response: Accept in principle**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

The guidance developed and published by the Office of the Privacy Commissioner should take into account relevant local and international standards, provided that such standards do not derogate from privacy protections afforded under the Privacy Act.

In regard to paragraph (f), it should be noted that the Government has already published the *Automated Assistance in Administrative Decision-Making: Better Practice Guide* (February 2007) (published jointly by the Australian Government Information Management Office, Australian National Audit Office, the Commonwealth Ombudsman and the Office of the Privacy Commissioner).

**Recommendation 10–4** The Office of the Privacy Commissioner should develop and publish guidance for organisations on the privacy implications of data-matching.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

## 11. Individuals, the Internet and Generally Available Publications

**Recommendation 11–1** The Office of the Privacy Commissioner should develop and publish guidance that relates to generally available publications in an electronic format. This guidance should:

- (a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;
- (b) set out the factors that agencies and organisations should consider before publishing personal information in an electronic format (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and
- (c) clarify the application of the model Unified Privacy Principles to the collection of personal information from generally available publications for inclusion in a record or another generally available publication.

### **Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

**Recommendation 11–2** The Australian Government should ensure that federal legislative instruments establishing public registers containing personal information set out clearly any restrictions on the electronic publication of that information.

### **Response: Not accept**

Given the potential scope of this recommendation and the existing standards followed by Commonwealth legislative drafters, the Government does not consider it necessary to implement this recommendation.



## PART C – INTERACTION, INCONSISTENCY AND FRAGMENTATION

### 15. Federal Information Laws

**Recommendation 15–1** The *Freedom of Information Act 1982* (Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act* is a disclosure that is required or authorised by or under law for the purposes of the ‘Use and Disclosure’ principle under the *Privacy Act*.

**Response: Not accept**

The Government considers that the release of personal information in accordance with the *Freedom of Information Act 1982* (FOI Act) is a disclosure that is required or authorised by or under law and is therefore a permitted disclosure under the *Privacy Act*.

The Government is of the view that disclosure under the FOI Act is a clear example of an action which is required or authorised by law and that it is unnecessary to amend the FOI Act to provide further certainty on this issue.

**Recommendation 15–2** 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*.

**Response: Accept**

On 5 August 2008, the Attorney-General issued a reference to the ALRC to review relevant laws and practices relating to the protection of Commonwealth information, including the scope and appropriateness of legislative provisions regarding secrecy and confidentiality. The ALRC is due to provide its report to the Attorney-General by 31 October 2009.

**Recommendation 15–3** Part VIII of the *Privacy Act* (Obligations of confidence) should be repealed.

**Response: Noted**

The ALRC has based this recommendation on the proviso that the Government enact a statutory cause of action for a serious invasion of privacy. The Government notes that it will consider its response to the statutory cause of action in its second stage consideration of the ALRC’s report and will therefore consider this recommendation as part of that response.

## 16. Required or Authorised by or Under Law

**Recommendation 16–1** The *Privacy Act* should be amended to provide that ‘law’, for the purposes of determining when an act or practice is required or authorised by or under law, includes:

- (a) Commonwealth, state and territory Acts and delegated legislation;
- (b) a duty of confidentiality under common law or equity (including any exceptions to such a duty);
- (c) an order of a court or tribunal; and
- (d) documents that are given the force of law by an Act, such as industrial awards.

### **Response: Accept in principle**

The Government broadly agrees with the proposed definition. However, given the inclusive nature of the definition, the Government does not agree that the reference to common law or equitable duties should be restricted to the duty of confidentiality. Instead a reference should be made to ‘common law or equitable duties’ in the proposed definition of ‘law’. In order to address concerns about the breadth of these duties, in particular, concerns that this will allow parties to contract out of obligations under the Privacy Act, the definition will specifically exclude contracts.

The Government also notes that while a definition will provide a degree of clarity, the meaning of ‘law’ within the required or authorised exception is best determined on a case-by-case basis. To determine whether a law, in whatever form, will allow an agency or organisation to conduct an action which is contrary to the Privacy Act it is necessary to consider:

- (i) whether or not the law applies to the agency or organisation; and
- (ii) whether the law actually requires or authorises the proposed act.

The Government considers these factors are important not only in determining the application of the exception but also in determining whether an applicable law is relevant under the Privacy Act.

**Recommendation 16–2** The Office of the Privacy Commissioner should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. This guidance should include:

- (a) a list of examples of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*; and
- (b) a note to the effect that the list is intended to be a guide only and that omission from the list does not mean that a particular law cannot be relied upon for the purposes of a ‘required or authorised by or under law’ exception in the model Unified Privacy Principles.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

**Recommendation 16–3** The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, state and territory privacy commissioners and agencies with responsibility for privacy regulation, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

**Response: Accept**

The Government is in favour of data-matching with strong privacy protections.

The Government encourages the development and publication of appropriate protocols by the Australian Electoral Commission and state and territory electoral commissions in order to establish more consistent privacy protections for the sharing of personal information for the continuous update of the electoral roll.

**Recommendation 16–4** The review under s 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) should consider, in particular, whether:

- (a) reporting entities and designated agencies are handling personal information appropriately under the legislation;
- (b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;
- (c) it remains appropriate that reporting entities are required to retain information for seven years;
- (d) the use of the electoral roll by reporting entities for the purpose of identification verification is appropriate; and
- (e) the handling of information by the Australian Transaction Reports and Analysis Centre is appropriate, particularly as it relates to the provision of access to other bodies, including bodies outside Australia.

**Response: Accept in principle**

The Government supports strong anti-money laundering and counter-terrorism financing laws that meet our international obligations.

The Government will consider the issues raised in this recommendation in its review of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* to the extent that they remain relevant and appropriate.

## PART D – THE PRIVACY PRINCIPLES

### 18. Structural Reform of the Privacy Principles

**Recommendation 18–1** The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:

- (a) the obligations in the privacy principles generally should be expressed as high-level principles;
- (b) the privacy principles should be technology neutral;
- (c) the privacy principles should be simple, clear and easy to understand and apply; and
- (d) the privacy principles should impose reasonable obligations on agencies and organisations.

**Response: Accept**

The Government strongly agrees with this recommendation.

**Recommendation 18–2** The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles, referred to in this Report as the model Unified Privacy Principles.

**Response: Accept**

The Government strongly supports reforming the Privacy Act to create a single set of Privacy Principles which will apply to both agencies and organisations, where appropriate.

## 19. Consent

**Recommendation 19–1** The Office of the Privacy Commissioner should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should:

- (a) address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained;
- (b) cover express and implied consent as it applies in various contexts; and
- (c) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

### **Response: Accept with amendment**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

In addition to accepting recommendation 19-1, the Government will expand the definition of 'consent' to clarify that an individual may withdraw consent where it is lawful to do so. When consent can be withdrawn 'lawfully' would include where it is in accordance with the principles of common or contractual law.

## 20. Anonymity and Pseudonymity

**Recommendation 20–1** The model Unified Privacy Principles should contain a principle called ‘Anonymity and Pseudonymity’ that requires an agency or organisation to give individuals the clear option to interact anonymously or pseudonymously, where this is lawful and practicable in the circumstances.

### **Response: Accept**

Giving individuals the option to interact anonymously or by using a pseudonym is an effective way to protect individuals’ privacy by ensuring that personal information is only collected where necessary.

This obligation should be limited to where it is lawful and practicable for agencies and organisations to allow anonymous or pseudonymous interaction.

**Recommendation 20–2** The Office of the Privacy Commissioner should develop and publish guidance on:

- (a) when it is and is not ‘lawful and practicable’ to give individuals the option to interact anonymously or pseudonymously with agencies or organisations;
- (b) what is involved in providing a ‘clear option’ to interact anonymously or pseudonymously; and
- (c) the difference between providing individuals with the option to interact anonymously and pseudonymously.

### **Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

Guidance on this issue will be very important in explaining that the right to interact anonymously or pseudonymously is limited to where it is lawful and practicable in the circumstances. For example, anonymous or pseudonymous interactions will usually not be practicable or lawful for the delivery and administration of many government services, benefits and entitlements, as well as in compliance, enforcement and investigative contexts.

## 21. Collection

**Recommendation 21–1** The model Unified Privacy Principles should contain a principle called ‘Collection’ that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.

### **Response: Accept**

The Government agrees that an agency or organisation should only collect personal information about an individual from that individual unless it is not reasonable and practicable to do so.

Collecting personal information directly from the individual can help to ensure the individual is aware their information has been collected. It can also assist in ensuring the personal information collected is accurate, complete and up-to-date.

The Government agrees with the ALRC that there will be many situations, particularly for agencies, where it will not be reasonable or practicable to collect personal information directly from the individual concerned. In such circumstances, the principle will not impose any requirement that personal information be collected directly from the relevant individual.

**Recommendation 21–2** The Office of the Privacy Commissioner should develop and publish further guidance to clarify when it would not be reasonable and practicable to collect personal information about an individual only from the individual concerned. In particular, the guidance should address collection:

- (a) of personal information by agencies pursuant to the exercise of their coercive information-gathering powers or in accordance with their intelligence-gathering, investigative, and compliance functions;
- (b) of statistical data;
- (c) of personal information in circumstances in which it is necessary to verify an individual’s personal information;
- (d) of personal information in circumstances in which the collection process is likely to, or will, disclose the personal information of multiple individuals; and
- (e) from persons under the age of 18, persons with a decision-making incapacity and those authorised to provide personal information on behalf of the individual.

### **Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

Guidance on this issue will be of particular importance in explaining those matters specified in paragraphs (a) to (e). Such guidance should recognise there are many circumstances where it will not be reasonable or practicable to collect personal information directly from an individual, particularly when personal information is collected by an agency.



**Recommendation 21–3** The ‘Collection’ principle should provide that, where an agency or organisation receives unsolicited personal information, it must either:

- (a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
- (b) comply with all relevant provisions in the model Unified Privacy Principles that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

**Response: Accept**

The Government agrees that personal information that is received by an agency or organisation should still be afforded privacy protections, even where the agency or organisation has done nothing to solicit the information.

If unsolicited personal information is not necessary for an agency or organisation’s functions or activities, it should be destroyed or de-identified where lawful and practicable to do so. This would apply to unsolicited information received by the organisation or agency from either the individual the information relates to or from any other third party.

If an agency or organisation is required, or decides, to retain unsolicited personal information, then it should comply with all of the Privacy Principles in respect of that information, as if the agency or organisation had taken active steps to collect the information.

In complying with the relevant Privacy Principles, an organisation or agency should properly consider the application of any qualifications or exceptions to those principles.

**Recommendation 21–4** The Office of the Privacy Commissioner should develop and publish guidance about the meaning of ‘unsolicited’ in the context of the ‘Collection’ principle.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

It would be important for such guidance to explain how this principle may apply to unsolicited personal information that is necessary for compliance, enforcement and regulatory functions, including where confidential ‘tip-offs’ are received.

The guidance should recognise that the requirement to comply with relevant Privacy Principles in respect of unsolicited personal information encompasses a consideration of any qualifications or exceptions to those principles. For example, the ‘notification’ principle provides that there are circumstances where it can be reasonable not to tell an individual that their personal information has been collected.

Guidance from the Office of the Privacy Commissioner would also clarify that the proposed principle does not affect the operation of the *Archives Act 1983* in relation to agencies.

**Recommendation 21–5** The ‘Collection’ principle in the model Unified Privacy Principles should provide that an agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

**Response: Accept**

Ensuring that personal information is only collected where necessary for a function or activity of an agency or organisation is an effective measure to protect privacy. The Government notes that an agency or organisation should be able to clearly identify the relevant functions or activities which it relies on to collect the information.

‘Necessary’ should be interpreted objectively and in a practical sense. If an agency or organisation cannot, in practice, effectively pursue a function or activity without collecting personal information, then that personal information would be regarded as necessary for that function or activity. An agency or organisation should not collect personal information on the off chance that it may become necessary for one of its functions or activities in the future, or that it may be merely helpful.

The Government notes that in addition to this requirement, agencies and organisations should only collect personal information by lawful and fair means and in a way that is not unreasonably intrusive.

## 22. Sensitive Information

**Recommendation 22–1** The model Unified Privacy Principles should set out the requirements of agencies and organisations in relation to the collection of personal information that is defined as ‘sensitive information’ for the purposes of the *Privacy Act*. These requirements should be located in the ‘Collection’ principle.

### Response: Accept

The Government agrees with the ALRC that the community expects ‘sensitive information’ to be afforded higher privacy protections than personal information that is not sensitive.

These protections should apply regardless of whether sensitive information is held by agencies or organisations.

These requirements include that sensitive information may not be collected except where permitted by specified exceptions. This requirement is applicable to unsolicited sensitive information.

In addition to the exceptions set out in recommendations 22-2 and 22-3, the collection of sensitive information should also be permitted:

- (i) where the relevant individual has consented;
- (ii) for the investigation of various matters that align with existing exceptions in National Privacy Principle (NPP) 2.1(f) and (h);
- (iii) for collection by non-profit organisations, subject to the conditions that align with NPP 10.1(d); or
- (iv) where necessary for a legal or equitable claim.

Items (i), (iii) and (iv) above mirror existing exceptions in NPP 2 and the proposed exceptions in the ALRC’s proposed Unified Privacy Principles.

**Recommendation 22–2** The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or authorised by or under law.

### Response: Accept

Sensitive information should be able to be collected by agencies or organisations where that collection is required or authorised by or under law.

**Recommendation 22–3** The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is legally or physically incapable of giving or communicating consent.

**Response: Accept in part**

Agencies and organisations should be permitted to collect sensitive information about an individual where the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, and it would be unreasonable or impracticable to obtain the individual's consent.

The fact that an individual lacks capacity to give consent, or is physically unable to communicate consent, would go to determining whether it is reasonable or practicable to seek consent.

As noted in the response to recommendation 25-3, the Government considers that, for consistency, a 'serious threat' should refer to 'life, health or safety'.

## 23. Notification

**Recommendation 23–1** The model Unified Privacy Principles should contain a principle called ‘Notification’ that sets out the requirements on agencies and organisations to notify individuals or otherwise ensure they are aware of particular matters relating to the collection and handling of personal information about the individual.

### Response: Accept

Notifying individuals about how their personal information will be handled is important to ensuring that they are fully informed and are able to make decisions about their personal information.

The Government supports, subject to amendment, the approach taken in recommendation 23-2 below.

**Recommendation 23–2** The ‘Notification’ principle should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify or otherwise ensure that the individual is aware of the:

- (a) fact and circumstances of collection where the individual may not be aware that his or her personal information has been collected;
- (b) identity and contact details of the agency or organisation;
- (c) rights of access to, and correction of, personal information provided by these principles;
- (d) purposes for which the information has been collected;
- (e) main consequences of not providing the information;
- (f) actual, or types of, agencies, organisations, entities or persons to whom the agency or organisation usually discloses personal information of the kind collected;
- (g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency’s or organisation’s Privacy Policy; and
- (h) fact, where applicable, that the collection is required or authorised by or under law.

### Response: Accept with amendment

The Government agrees the proposed ‘notification’ principle should provide that there may be circumstances where it is reasonable to take no steps to notify an individual about the collection of their personal information. These circumstances include those matters specified under recommendation 23-3, about which the Office of the Privacy Commissioner would be encouraged to provide guidance.

On recommendation 23-2(a), the Government notes that this information need only be provided in specific circumstances. Accordingly, the intent of this principle may be better expressed by reversing the clause so that the specified matter is: ‘where the individual may not be aware that his or her personal information has been collected, the fact and

circumstances of collection’.

On recommendation 23-2(h), agencies or organisations should identify the specific law that requires or authorises the collection of information, though it would not be necessary to identify a specific provision.

The Government notes community concern regarding the flow of personal information overseas. Accordingly, in addition to the matters specified in recommendation 23-2, agencies and organisations should also take such steps, if any, as are reasonable in the circumstances to notify individuals if their personal information is reasonably likely to be transferred overseas and to where it may be transferred.

This requirement would be qualified by the ‘reasonable steps’ test. For example, an agency or organisation would not need to include this information in a collection notice if it did not reasonably know at the time of collection whether information will be transferred overseas.

Further, it would not be reasonable to provide specific information if the organisation or agency does not reasonably know to which specific jurisdiction personal information may be transferred.

**Recommendation 23–3** The Office of the Privacy Commissioner should develop and publish guidance to assist agencies and organisations in complying with the ‘Notification’ principle. In particular, the guidance should address:

- (a) the circumstances when it would and would not be reasonable for an agency or organisation to take no steps to notify individuals about the matters specified in the ‘Notification’ principle. In this regard, the guidance should address the circumstances when:
  - (i) notification would prejudice the purpose of collection, for example, where it would prejudice:
    - the prevention, detection, investigation, and prosecution of offences, breaches of law imposing a penalty or seriously improper conduct;
    - the enforcement of laws; or
    - the protection of the public revenue;
  - (ii) the collection of personal information is required or authorised by or under law for statistical or research purposes;
  - (iii) the personal information is collected from an individual on repeated occasions;
  - (iv) an individual has been made aware of the relevant matters by the agency or organisation which disclosed the information to the collecting agency or organisation;
  - (v) non-compliance with the principle is authorised by the individual concerned;
  - (vi) the taking of no steps is required or authorised by or under law;
  - (vii) notification would pose a serious threat to the life or health of any individual; and
  - (viii) health services collect family, social or medical histories;
- (b) the appropriate level of specificity when notifying individuals about anticipated disclosures to agencies, organisations, entities and persons; and
- (c) the circumstances in which an agency or organisation can comply with specific limbs of the ‘Notification’ principle by alerting an individual to specific sections of its Privacy

Policy or to other general documents.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

This guidance would be important in clarifying that the intent of the principle is to promote consumer awareness and trust in how agencies and organisations handle personal information, and that the principle should not be interpreted in such a way as to impose unnecessary regulatory burden.

## 24. Openness

**Recommendation 24–1** The model Unified Privacy Principles should contain a principle called ‘Openness’. The principle should set out the requirements on an agency or organisation to operate openly and transparently by setting out clearly expressed policies on its handling of personal information in a Privacy Policy, including how it collects, holds, uses and discloses personal information. This document also should include:

- (a) what sort of personal information the agency or organisation holds;
- (b) the purposes for which personal information is held;
- (c) the steps individuals may take to access and correct personal information about them held by the agency or organisation; and
- (d) the avenues of complaint available to individuals in the event that they have a privacy complaint.

### **Response: Accept with amendment**

The Government agrees that organisations and agencies should consider their personal information handling policies and practices and clearly set these out in a Privacy Policy available to all individuals. This helps to promote transparency in the handling of personal information, as well as consumer control, choice and trust in how their information will be handled.

The Government also agrees that requiring agencies and organisations to express in their Privacy Policies how they handle personal information at each stage of the information cycle, will encourage them to consider how the Privacy Principles apply to their activities.

Consistent with the ALRC’s proposed model Unified Privacy Principle 4.1(e) and recommendation 31-8, a Privacy Policy should also outline whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.

The ‘openness’ principle should reflect the diverse characteristics of agencies and organisations, and the potential differences in information handling practices, by specifying a non-exhaustive range of matters for inclusion in Privacy Policies. Where agencies or organisations have particularly significant information handling practices, these should be included in their Privacy Policies by clearly setting out how they collect, hold, use and disclose personal information. For example, where agencies or organisations have specific information retention or destruction obligations, these should be described as a necessary part of how they handle personal information.

#### ***Requirement to maintain the Privacy Policy***

To reflect that information handling practices may change over time, the ‘openness’ principle should require agencies and organisations to ‘maintain’ their Privacy Policy by updating the document if policies and practices change. This recognises a Privacy Policy is a living document and that information handling policies should be kept under review.

#### ***Role of the ‘openness’ principle in the information cycle***

The Government notes the ALRC’s intention to align the order of the Privacy Principles with the stages of the information handling cycle. As noted above, a Privacy Policy should express an agency or organisation’s consideration of how it handles personal information at each stage of the information cycle, and how the Privacy Principles apply to its activities. This consideration of information handling needs and practices should ideally occur before personal information is collected, that is, at the beginning of the information cycle. To reflect



this, the 'openness' principle should therefore be the first enumerated privacy principle.

***Requirement to implement compliance measures***

A Privacy Policy is intended to communicate to the public an agency or organisation's expressed information handling policies and practices. However, this document will be of little value if it does not reflect internal compliance measures and practices implemented by the agency or organisation.

In addition to the obligations proposed by the ALRC, the 'openness' principle should also require agencies and organisations to take reasonable steps, having regard to the circumstances of the agency or organisation, to develop and implement internal policies and practices that enable compliance with the Privacy Principles. These policies and practices could include:

- (i) training staff and communicating to staff information about the agency or organisation's policies and practices;
- (ii) establishing procedures to receive and respond to complaints and inquiries;
- (iii) developing information to explain the agency or organisation's policies and procedures; and
- (iv) establishing procedures to identify and manage privacy risks and compliance issues, including in designing and implementing systems or infrastructure for the collection and handling of personal information by the agency or organisation.

This additional requirement is intended to strengthen the 'openness' principle, by recognising that the publicly available Privacy Policy should be grounded in the actual internal policies and practices of the agency or organisation.

The underlying emphasis of the 'openness' principle is on the process of the agency or organisation considering how it handles personal information at each stage of the information cycle and how the Privacy Principles apply to its activities. As noted by the ALRC, this process may assist agencies and organisations to structure their operations so as to comply with the Privacy Principles.

Developing and implementing internal policies and procedures to enable compliance with the Privacy Principles, and developing a publicly available Privacy Policy, would both be outputs from the same process of consideration. However, the Privacy Policy would be communicating general information on how the agency or organisation manages personal information (providing transparency of personal information-handling practices), which may not always require the same level of detail as internal policies and practices.

The Government is of the view that this process of considering information handling and privacy compliance requirements needs to be encouraged further, by giving greater recognition in the Privacy Principles to the need for a proactive approach to privacy compliance.

This additional obligation would be a general obligation to take reasonable steps to implement policies and practices that try to ensure compliance with the Privacy Principles. It would not diminish the overriding obligation in the Privacy Act not to breach the Privacy Principles.

The specific policies and practices identified above in paragraphs (i) to (iv) are basic policies or practices that most agencies and organisations would need to implement to enable compliance. However, the obligation to implement such policies and practices would be qualified by a 'reasonable steps' test, as well as having regard to the circumstances of the agency or organisation, recognising that the appropriate steps to take will depend upon the circumstances of each agency or organisation.

In this way, the additional requirement adopts a risk-based approach, whereby an agency or organisation would consider what internal practices and policies to implement with regard to such matters as the volume of personal information it handles, the sensitivity of that information and the purpose for which the information is collected, used and disclosed.

In addition to considering the level of risk in their information handling needs and practices, agencies and organisations would also consider what is reasonable for them to do with regard to their size and available resources, the type of functions or activities they undertake, and the extent to which they have already established internal policies and practices.

This additional supporting obligation to the 'openness' principle would expressly recognise what is only implicit in the existing Privacy Principles: that agencies and organisations need to take positive steps to ensure they comply with the Privacy Principles. However, it reflects what many agencies and organisations currently do in practice to ensure they meet their obligations under the Privacy Act. It is therefore not intended to impose any unreasonable additional burden on agencies and organisations.

### **Guidance**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

Guidance on the 'openness' principle, in particular the additional requirements outlined above, would be important in assisting agencies and organisations to understand the nature and scope of the principle.

**Recommendation 24–2** An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the 'Openness' principle, available without charge to an individual electronically; and, on request, in hard copy or in an alternative form accessible to individuals with special needs.

### **Response: Accept**

The free availability of a Privacy Policy in the most appropriate form is essential to informing individuals how their personal information may be handled.

**Recommendation 24–3** The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information-handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

Short form privacy notices can provide a practical way to promote openness and transparency in how personal information may be handled.

The Office of the Privacy Commissioner should also provide guidance on the general application of the ‘openness’ principle.

## 25. Use and Disclosure

**Recommendation 25–1** The model Unified Privacy Principles should contain a principle called ‘Use and Disclosure’ that sets out the requirements on agencies and organisations in respect of the use and disclosure of personal information for a purpose other than the primary purpose of collection.

### **Response: Accept**

Appropriate limits on the use and disclosure of personal information by agencies and organisations provide important privacy protections.

These requirements should be balanced so as to recognise other important public interests that may, on occasion, compete with the public interest in maintaining the individual’s privacy.

Harmonising the requirements that apply to how agencies and organisations may use or disclose personal information is an essential element in promoting consistent and simple privacy regulation.

**Recommendation 25–2** The ‘Use and Disclosure’ principle should contain an exception permitting an agency or organisation to use or disclose an individual’s personal information for a purpose other than the primary purpose of collection (the secondary purpose), if the:

- (a) secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the primary purpose of collection; and
- (b) individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.

### **Response: Accept with amendment**

The Government agrees with recommendation 25-2.

In addition to the exceptions provided in this recommendation and in recommendation 25-3, agencies and organisations should also be permitted to use or disclose personal information for certain purposes other than the purpose for which it was initially collected.

These other exceptions include:

- (i) where the individual consents to the use or disclosure;
- (ii) where unlawful activity or serious misconduct is suspected and the agency or organisation uses or discloses personal information as a necessary part of its own investigation of the matter or in reporting its concerns to relevant persons or authorities;
- (iii) where the use or disclosure is required or authorised by or under law; and
- (iv) where the organisation or agency reasonably believes that the use or disclosure is reasonably necessary for the prevention, investigation, detection or prosecution of breaches of a law by or on behalf of an enforcement body.

Items (i) to (iv) above mirror existing exceptions in National Privacy Principle 2 and the proposed exceptions in the ALRC’s model Unified Privacy Principles.

Further, additional exceptions should provide for those matters addressed in the Government response to the following recommendations:

- (v) recommendation 44-1, where the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process;
- (vi) recommendations 65-2, 65-4, 65-5 and 65-9 concerning the use and disclosure of personal information for research purposes; and
- (vii) recommendations 63-3, 63-5 and 63-9 concerning the use and disclosure of personal information for the purpose of providing a health service.

***Use and disclosure for the purpose of locating missing persons***

The Government notes the ALRC considered but declined to recommend that agencies and organisations should be permitted to use or disclose personal information for the purpose of locating a reported missing person. The ALRC did not find that such an exception was necessary, arguing that other exceptions, including the revised 'serious threat' exception, could be relied on in many cases.

While the Government agrees that using or disclosing personal information to locate missing persons may often be permitted by other exceptions, it is of the view that an express exception should also apply for those instances where the application of other exceptions is unclear.

The Government recognises the particular sensitivity that may attach to the personal information of individuals who have been reported missing. Such individuals may have exercised their free choice to disassociate themselves from friends and family for legitimate reasons, including removing themselves from harmful environments. Therefore, it is appropriate that any discretion for agencies and organisations to use or disclose personal information about reported missing persons should not be unfettered.

Accordingly, the 'use and disclosure' principle should include an exception that permits, though does not require, agencies or organisations to use or disclose personal information where necessary for the purpose of locating reported missing persons. Any such uses or disclosures should be in accordance with binding rules issued by the Privacy Commissioner. These rules will be in the form of a legislative instrument and therefore subject to the scrutiny of Parliament.

Matters which the Privacy Commissioner's rules should address include:

- that uses and disclosures should only be in response to requests from appropriate bodies with recognised authority for investigating reported missing persons;
- that, where reasonable and practicable, the individual's consent should be sought before using or disclosing their personal information;
- where it is either unreasonable or impracticable to obtain consent from the individual, any use or disclosure should not go against any known wishes of the individual;
- disclosure of personal information should be limited to that which is necessary to offer 'proof of life' or contact information; and
- agencies and organisations should take reasonable steps to assess whether disclosure would pose a serious threat to any individual.

Consistent with the requirements of the *Legislative Instruments Act 2003*, the Privacy Commissioner should consult with relevant stakeholders in making these rules.

**Recommendation 25–3** The ‘Use and Disclosure’ principle should contain an exception permitting an agency or organisation to use or disclose an individual’s personal information for a purpose other than the primary purpose of collection (the secondary purpose) if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual’s life, health or safety; or (b) public health or public safety.

**Response: Accept with amendment**

The Government accepts the ‘use and disclosure’ principle should include an exception allowing use or disclosure where an agency or organisation reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to: (a) an individual’s life, health or safety; or (b) public health or public safety.

The Government notes that this recommendation removes the current requirement in the equivalent principles that a serious threat also be imminent. The Government agrees that the test of ‘imminence’ can be too restrictive.

At the same time, the Government recognises the concerns of a number of stakeholders that the removal of the ‘imminence’ requirement would excessively broaden the exception and remove an important safeguard against the mishandling of personal information.

Accordingly, the Government has determined that a compromise position should be pursued, which is less restrictive than currently applied, though prevents excessive broadening of the exception.

Agencies and organisations should be permitted to use or disclose personal information in the circumstances set out in the recommendation only after consent has first been sought, where that is reasonable and practicable.

For the purposes of this exception, whether it was ‘reasonable’ to seek consent would include whether it is realistic or appropriate to seek consent. This might include whether it could be reasonably anticipated that the individual would withhold consent (such as where the individual has threatened to do something to create the serious risk). It would also likely be unreasonable to seek consent if there is an element of urgency that required quick action. Whether the individual had, or could be expected to have, capacity to give consent would also be a factor in determining whether it was ‘reasonable’ to seek consent.

Seeking consent would not be ‘practicable’ in a range of contexts. These could include when the individual’s location is unknown or they cannot be contacted. If seeking consent would impose a substantial burden then it may not be practicable. It may also not be practicable to seek consent if the use or disclosure relates to the personal information of a very large number of individuals.

In assessing whether it is ‘reasonable or practicable’ to seek consent, agencies and organisations could also take into account the potential consequences and nature of the serious threat.

This approach creates a presumption that agencies and organisations should consider seeking consent before using or disclosing personal information in the circumstances set out in the recommendation.

The Government notes that this amended exception will also apply to the collection of sensitive information under the proposed ‘collection’ principle.

The Government notes that several Privacy Principles provide for collection, use or disclosure of personal information where there is a ‘serious threat’. However, there are differences across the existing National Privacy Principles and the ALRC’s

recommendations as to whether the 'serious threat' relates to 'life or health' or 'life, health or safety'. The Government considers there should be consistency across the Privacy Principles and that the 'safety' of individuals and third parties should be included as a relevant consideration in relation to serious threats. See also recommendations 22-3, 29-3, 63-5 and 63-6, which all refer to a 'serious threat'.

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner. Guidance from the Office of the Privacy Commissioner on the application of this recommendation would be important in assisting agencies and organisations to understand their obligations.

## 26. Direct Marketing

**Recommendation 26–1** The model Unified Privacy Principles should regulate direct marketing by organisations in a discrete privacy principle, separate from the ‘Use and Disclosure’ principle. This principle should be called ‘Direct Marketing’ and it should apply regardless of whether the organisation has collected the individual’s personal information for the primary purpose or a secondary purpose of direct marketing. The principle should distinguish between direct marketing to individuals who are existing customers and direct marketing to individuals who are not existing customers.

### **Response: Accept with amendment**

The Government agrees that a separate principle should regulate the use and disclosure of personal information for the purpose of direct marketing. This will provide greater clarity regarding the regulation of personal information for such activities. Applying different standards to individuals who have an established relationship with an organisation and those individuals who do not, appropriately reflects the level of concern individuals may have about how their personal information is handled in each case.

Some stakeholders have expressed the view that the ‘direct marketing’ principle should extend to agencies. The Government agrees with the ALRC that this would generally not be appropriate.

However, the Government notes that section 7A of the Privacy Act provides that acts of certain agencies are to be treated as the acts of organisations. The policy intent of section 7A is that bodies operating in the commercial sphere should operate on a level playing field. Where agencies are engaged in commercial activities, they should be required to comply with the Privacy Principles just like private sector organisations. A note should accompany the ‘direct marketing’ principle that draws attention to the role of section 7A.

Additionally, the Government notes that individuals may have a broad range of relationships with different types of organisations. The term ‘customer’ might not best characterise the relationship in all contexts. Accordingly, ‘customer’ should be construed in a broad sense to recognise the types of relationships individuals may have with a range of organisations, including social groups and clubs, charities, religious organisations and private educational institutions, each of which may conduct direct marketing. The Government will seek the advice of the Office of Parliamentary Counsel about reflecting this intent in the amendment legislation.



**Recommendation 26–2** The ‘Direct Marketing’ principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.

**Response: Accept**

The Government agrees that the general requirements of the ‘direct marketing’ principle should be displaced by more specific sectoral legislation that regulates the handling of personal information for direct marketing.

The relationship between the Privacy Act, *Spam Act 2003* and *Do Not Call Register Act 2006* can result in unnecessary complexity in the regulation of personal information for different forms of direct marketing. Recommendation 26-2 will assist in resolving this potential complexity.

**Recommendation 26–3** The ‘Direct Marketing’ principle should provide that an organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:

- (a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and
- (b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications.

**Response: Accept with amendment**

The Government agrees that organisations should be permitted to use or disclose personal information for the purpose of direct marketing to existing customers in accordance with the obligations set out in paragraphs (a) and (b) of the recommendation.

In addition, recommendation 26-4(a)(i) states that personal information that falls within the class of defined ‘sensitive information’ should only be used or disclosed for direct marketing to individuals who are not existing customers or who are under 15 years of age with their consent.

The Government believes that sensitive information, including health information, should only be used or disclosed for direct marketing purposes with the individual’s consent in all circumstances, including where the individual is an existing customer of an organisation.

The Government recognises that some individuals, including some children under 15 years of age, may be less able than others to appropriately recognise commercial influence.

The Government notes that concerns have been raised about the potential effect of certain types of direct marketing on children, particularly via email and SMS. The provisions of the Privacy Act, in effect, primarily relate to postal direct marketing. Direct marketing via means such as email and SMS is regulated by the *Spam Act 2003*.

There is insufficient evidence that postal direct marketing to young people has resulted in substantial adverse consequences.

Recommendation 26-3 would also establish an obligation for all organisations that conduct direct marketing to know if an individual is 15 years of age or older. The organisation may

not currently collect this information, nor need it for any other purpose. Therefore, this approach would likely result in the undesirable outcome of more personal information being collected about individuals than is otherwise necessary.

Accordingly, the Government is not convinced that there is sufficient justification for distinguishing direct marketing obligations on the basis of an individual's age. Such a measure would impose an unnecessary regulatory burden and added complexity, without substantial benefit.

**Recommendation 26—4** The 'Direct Marketing' principle should provide that an organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:

- (a) either:
  - (i) the individual has consented; or
  - (ii) the information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;
- (b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays, a notice advising the individual that he or she may express a wish not to receive any direct marketing communications; and
- (c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications.

**Response: Accept in part**

The Government agrees that individuals who are not existing customers of an organisation should be told they can opt-out of their personal information being used for direct marketing and that such a right should be simple to exercise.

In line with the Government's response to recommendation 26-3, the Government does not agree that an age-based distinction should be incorporated in the principle.

**Recommendation 26–5** The ‘Direct Marketing’ principle should provide that an organisation involved in direct marketing must comply, within a reasonable period of time, with an individual’s request not to receive further direct marketing communications and must not charge the individual for giving effect to such a request.

**Response: Accept with amendment**

The Government agrees that organisations should be obliged to stop using or disclosing personal information for the purpose of direct marketing where requested by an individual.

There should be no charge for giving effect to such a request, nor should there be any charge for making such a request.

This obligation should extend to any organisation that uses or discloses personal information to send or to facilitate the sending of direct marketing. This includes any organisation who is identified as the ‘source’ of personal information which facilitated the direct marketing. (Note recommendation 26-6 requires that individuals be told of the ‘source’ of their information when they receive direct marketing from an organisation of which they are not an existing customer).

**Recommendation 26–6** The ‘Direct Marketing’ principle should provide that an organisation that has made direct marketing communications to an individual who is not an existing customer or is under 15 years of age must, where reasonable and practicable and where requested to do so by the individual, advise the individual of the source from which it acquired the individual’s personal information.

**Response: Accept with amendment**

The Government agrees that individuals should have a right to be told the specific source from which their personal information was obtained when they are contacted by an organisation with which they have not had a customer relationship. This obligation should apply where practicable for the organisation.

This recommendation should be read in conjunction with recommendation 26-5, where the Government has indicated that individuals should also have the right to ask the organisation who is the relevant source not to use or disclose the individual’s personal information for direct marketing, including to facilitate direct marketing.

In line with the Government’s response to recommendation 26-3, the Government does not agree that an age-based distinction should be incorporated in the principle.

**Recommendation 26–7** The Office of the Privacy Commissioner should develop and publish guidance to assist organisations in complying with the ‘Direct Marketing’ principle, including:

- (a) what constitutes an ‘existing customer’;
- (b) the types of direct marketing communications which are likely to be within the reasonable expectations of existing customers;
- (c) the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing to an individual who is not an existing customer or is under the age of 15 years;
- (d) the factors for an organisation to consider in determining whether it is reasonable and practicable to advise an individual of the source from which it acquired the individual’s personal information; and
- (e) the obligations of organisations involved in direct marketing under the *Privacy Act* in dealing with vulnerable people.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

In relation to paragraph (c), the Government notes that, in line with the Government’s response to recommendation 26-3 regarding the use of an age-based distinction for different direct marketing obligations, it will not be necessary for the Office of the Privacy Commissioner to provide guidance on the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing to an individual under the age of 15 years.

## 27. Data Quality

**Recommendation 27–1** The model Unified Privacy Principles should contain a principle called ‘Data Quality’ that requires an agency or organisation to take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

### **Response: Accept**

Agencies and organisations should take reasonable steps to make certain that the personal information they collect, use or disclose is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

This requirement would apply at the time of collection, use and disclosure. As it would be qualified by a ‘reasonable steps’ requirement and assessed by reference to the purpose of collection, use or disclosure, it would be reasonable to take no steps in some circumstances, reflecting the intended proportional approach to compliance with this principle.

It would be helpful for the Office of the Privacy Commissioner to publish guidance on the application of the ‘data quality’ principle. This could include guidance on what may constitute ‘reasonable steps’ for the purposes of the principle.

## 28. Data Security

**Recommendation 28–1** The model Unified Privacy Principles should contain a principle called ‘Data Security’ that applies to agencies and organisations.

**Response: Accept**

The ‘data security’ principle should require an agency or organisation to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

The ‘data security’ principle should also contain the matters set out in recommendation 28-4.

**Recommendation 28–2** A note should be inserted after the ‘Data Security’ principle cross-referencing to the data breach notification provisions.

**Response: Noted**

It would be premature to accept this recommendation in advance of the Government considering the ALRC’s recommendations regarding data breach notification provisions.

This recommendation should be considered in the second stage of the Government’s response to the ALRC’s report.

**Recommendation 28–3** The Office of the Privacy Commissioner should develop and publish guidance about the ‘reasonable steps’ agencies and organisations should take to prevent the misuse and loss of personal information. This guidance should address matters such as the:

- (a) factors that should be taken into account in determining what are ‘reasonable steps’, including: the likelihood and severity of harm threatened; the sensitivity of the information; the cost of implementation; and any privacy infringements that could result from such data security steps; and
- (b) relevant security measures, including privacy-enhancing technologies such as encryption, the security of paper-based and electronic information, and organisational policies and procedures.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

**Recommendation 28–4** (a) The ‘Data Security’ principle should require an agency or organisation to take reasonable steps to destroy or render non-identifiable personal information if:

- (i) it is no longer needed for any purpose for which it can be used or disclosed under the model Unified Privacy Principles; and
- (ii) retention is not required or authorised by or under law.

(b) The obligation to destroy or render non-identifiable personal information is not ‘required by law’ for the purposes of s 24 of the *Archives Act 1983* (Cth).

**Response: Accept**

Keeping personal information for only as long as is reasonably necessary is an effective way of reducing the risk that it may be mishandled.

This recommendation does not affect the operation of the *Archives Act 1983* on how agencies retain personal information.

**Recommendation 28–5** The Office of the Privacy Commissioner should develop and publish guidance about the destruction of personal information, or rendering such information non-identifiable. This guidance should address matters such as:

- (a) when it is appropriate to destroy or render non-identifiable personal information, including personal information that:
  - (i) forms part of a historical record; and
  - (ii) may need to be preserved, in some form, for the purpose of future dispute resolution;
- (b) the interaction between the data destruction requirements and legislative records retention requirements; and
- (c) the manner in which personal information should be destroyed or rendered non-identifiable.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

## 29. Access and Correction

**Recommendation 29–1** The model Unified Privacy Principles should contain a principle called ‘Access and Correction’ that, subject to Recommendation 29–2, applies consistently to agencies and organisations.

### **Response: Accept**

The Government agrees that an individual’s rights of access and correction to his or her own personal information held by agencies and organisations should, to the extent possible, be provided for under a single principle.

The Government notes the implications this raises for the interaction between the Privacy Act and the *Freedom of Information Act 1982* (FOI Act), and makes the following additional comments on the proposed approach to this interaction between the two Acts.

#### ***Enforceable right of access and correction in the Privacy Act***

As part of its proposed reforms to the FOI Act, the Government announced on 24 March 2009 a proposal to amend the Privacy Act to enact an enforceable right of access to, and correction of, an individual’s own personal information, rather than maintain this right through the FOI Act.

The proposed ‘access and correction’ principle will provide this enforceable right. Consistent with the culture of pro-disclosure of Government information the FOI Act reforms seek to promote, the proposed Privacy Act reforms will seek to facilitate easier access and correction to an individual’s own personal information held by agencies. In this regard, the Government agrees that the Privacy Act should provide a simple and user-friendly mechanism for individuals to access and correct their own personal information.

#### ***Single privacy principle to provide for access and correction***

In creating a unified set of Privacy Principles applying to both the public and private sectors alike, the Government agrees that an individual’s rights of access and correction to his or her own personal information held by agencies and organisations should, to the extent possible, be provided for under a single principle.

However, it will be necessary for the ‘access and correction’ principle to recognise the additional responsibilities of Government in relation to disclosures of some categories of information and documents (such as documents affecting national security, defence or international relations). The Privacy Act should not allow individuals to obtain access to information that would not otherwise be able to be accessed under the FOI Act or other applicable Commonwealth laws.

#### ***Privacy Act to provide primary avenue for access and correction rights***

The existing overlap between the FOI Act and Privacy Act has been interpreted as making the FOI Act the primary avenue for individuals to access and correct their own personal information held by agencies.

The Government proposes that guidance and legislative amendment make clear that the Privacy Act is the primary avenue for access to, and correction of, an individual’s own personal information. These changes are intended to make the Privacy Act the key Commonwealth law for the collection, handling, disclosure and accessing of personal information. As a result, the focus of the FOI Act is intended to be on access to documents held by government other than an individual’s own personal information.

However, in recognition that there will be circumstances where documents held by agencies contain a mixture of: (a) an individual’s personal information; (b) the personal information of



third parties; and (c) non-personal information, in such a way as to make it difficult to release only the individual's personal information, or that individuals may make access requests for files that contain such a mixture of information, the Government agrees that rights to access some personal information should be retained under the FOI Act. Agencies will need to establish administrative processes for dealing with the different access and correction requests that will arise under the Privacy and FOI Acts, having regard to the types of records and information they hold. As noted below, guidance on the interaction between the two Acts will be critical for agencies.

### ***Correction rights – FOI Act amendments***

As with the access rights, the existing rights of amendment and annotation are proposed to be retained in the FOI Act to allow for the circumstances outlined above. Given the differences between the correction and annotation rights available under the Privacy and FOI Acts that currently exist, the Government proposes to amend the FOI Act to achieve greater consistency of these rights between the two Acts. This would implement recommendations from the joint ALRC and Administrative Review Council report *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995).

### ***Enforcement and review rights***

The proposed 'access and correction' principle will provide individuals with an enforceable right of access and correction through the complaints process to the Privacy Commissioner.

Some stakeholders have expressed concerns that, with the Privacy Act taking over from the FOI Act to provide individuals with access and correction of their own personal information held by agencies, the Privacy Act should provide equivalent rights of review as are available under the FOI Act in relation to agency decisions on granting access or making corrections.

Under the FOI Act, agency decisions about access and correction can be subject to internal review by the agency as well as external review by the Administrative Appeals Tribunal (AAT). Reforms to the FOI Act and the establishment of the Office of the Information Commissioner (OIC) will also provide for the ability to have an initial external review by the Information Commissioner before AAT review.

The intention is for processes around reviews of agency access and correction decisions under the Privacy Act to align as closely as possible with reviews of access and correction decisions under the FOI Act, in line with the proposed operation of the OIC.

As part of this, the Government proposes that, for complaints from individuals about an agency's decision to refuse access, or correction of, personal information, the Privacy Commissioner will be required to review the agency's decision and make a decision on the review (affirming, varying or substituting the agency's decision). This review process for access and correction complaints will not apply more generally in respect of complaints about agencies' acts or practices relating to other Privacy Principles.

Complaints from individuals about an organisation's decision to refuse access to their personal information will be dealt with under the general complaint handling processes applying to complaints relating to other Privacy Principles, including conciliation and the option of the Commissioner making a determination. The Government notes the proposal in its response to recommendation 49-5, that there should be an ability for individuals to make an application directly to the Federal Court alleging interference with their privacy where they are not satisfied with a conciliated outcome or a decision of the Privacy Commissioner to decline to investigate, or investigate further, their complaint.

### ***Privacy Policy – outline access and correction rights***

Agencies and organisations would be required by the proposed 'openness' principle to develop and publish a Privacy Policy, setting out how they collect, hold, use and disclose personal information (see recommendation 24-1). This will include outlining the steps

individuals may take to gain access to and correct their personal information. As part of such policies, agencies could outline their administrative processes for responding to access and correction requests under both the Privacy and FOI Acts.

### **Guidance**

The Government notes recommendation 29-9 and emphasises that guidance will be critical in clarifying the interaction of rights of access and correction under the 'access and correction' principle in the Privacy Act with the rights of access and correction to be retained under the FOI Act.

### **Office of the Information Commissioner – FOI and Privacy co-located**

The Government's proposed FOI reforms include establishing a new Office of the Information Commissioner that will bring together an Information Commissioner, an FOI Commissioner and the Privacy Commissioner. The co-location of FOI and Privacy in this new structure will strengthen and elevate the role and importance of privacy laws.

In particular, this co-location will assist in the development of guidance and policy on issues relating to the interaction between the two Acts, and contribute to efforts to ensure individuals are able to obtain access to their own personal information through simple and user-friendly processes.

### **Future review**

As part of the Government's proposed reforms to the FOI Act, the Government committed to undertake a comprehensive review of the FOI Act two years after the commencement of the FOI reform legislation. This review could provide an opportunity to consider how the interaction between the Privacy Act and FOI Act is developing.

**Recommendation 29–2** The 'Access and Correction' principle should provide that:

- (a) if an agency holds personal information about an individual, the individual concerned is entitled to have access to that personal information, except to the extent that the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; and
- (b) subject to Recommendation 29–3, if an organisation holds personal information about an individual, the individual concerned shall be entitled to have access to that personal information, except to the extent that one of the exceptions to the right of access presently set out in National Privacy Principle 6.1 or 6.2 applies.

### **Response: Accept**

The Government agrees that the 'access and correction' principle should provide different exceptions to an individual's right of access, depending on whether the information is held by an agency or organisation. In relation to whether personal information is 'held', the principle should include information in the constructive possession of an agency or organisation.

The exceptions applying to Government agencies should be consistent with exceptions under the *Freedom of Information Act 1982* (FOI Act) and the *Archives Act 1983* (Archives Act). Individuals should not be able to compel access to information under the Privacy Act that would otherwise be exempt under the FOI Act, Archives Act or other applicable Commonwealth laws.

The Government's proposed reforms to the FOI Act are intended to modernise the

legislation. The streamlined provisions of the FOI Act may assist agencies in their consideration of the exemptions when responding to access requests under the 'access and correction' principle.

The Government recognises that guidance and legislative amendment will be required to clarify how the exemptions in the FOI Act and other applicable Commonwealth laws will be applied to access requests under the Privacy Act (see recommendation 29-9).

**Recommendation 29–3** The 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual, it is not required to provide access to the information to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of any individual.

**Response: Accept with amendment**

The Government agrees that individuals should not be entitled to obtain access to personal information that an organisation holds about them if providing access would pose a serious threat to the life or health of any individual (including the individual seeking access).

As noted in the response to recommendation 25-3, the Government considers that, for consistency, a 'serious threat' should refer to 'life, health or safety'.

The Government notes that this recommendation removes the current requirement in the equivalent principle (National Privacy Principle 6.1(a)) that a serious threat also be imminent. In recommendations 22-3 and 25-3 the ALRC has proposed that this 'imminence' requirement also be amended in the context of the proposed 'collection' and 'use and disclosure' principles. The Government notes that the amendments it has proposed in response to those recommendations would not be applicable in the context of the 'access and correction' principle.

In accepting this recommendation, the Government acknowledges the importance of the obligation outlined in recommendation 29-4 that agencies and organisations should take reasonable steps to provide individuals with access to as much information as possible, as an alternative to complete denial of access where an exception applies (recognising that this may not be possible in all circumstances).

**Recommendation 29–4** The 'Access and Correction' principle should provide that, where an agency or organisation is not required to provide an individual with access to his or her personal information, the agency or organisation must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.

**Response: Accept**

The Government agrees that the 'access and correction' principle should include a strengthened requirement to enable individuals to have access to their personal information to the greatest extent possible.

An agency or organisation's consideration of whether an exception applies should be followed by a proper consideration of whether some form of access can nevertheless be provided, notwithstanding it may be in a reduced form or indirect manner. Although there

will be some circumstances where access can legitimately be denied in its entirety, the existence of grounds to refuse access to some personal information should not always provide grounds for complete denial of access.

The Government emphasises that this requirement would be based on taking 'reasonable steps' to provide access, recognising there will be circumstances where it is reasonable to take no steps to provide access.

For example, where an agency is investigating unlawful activity, taking no steps to provide access may be appropriate if anything other than a complete refusal of the individual's access request would undermine the investigation. However, access requests would need to be considered on a case-by-case basis.

Guidance from the Office of the Privacy Commissioner will be important for assisting agencies and organisations to comply with this requirement (see recommendation 29-9). Such guidance could outline other means of providing access in addition to the use of a mutually agreed intermediary. For example, providing a verbal summary of information in a document or an edited copy of the document, excluding the information covered by the exception.

It is important to note that this provision would not be intended to provide a mechanism to reduce access if access would otherwise be required (consistent with the expressed intent of National Privacy Principle 6.3).

**Recommendation 29–5** The 'Access and Correction' principle should provide that, if an individual seeks to have personal information corrected under the principle, an agency or organisation must take such steps, if any, as are reasonable to:

- (a) correct the personal information so that, with reference to a purpose for which the information is held, it is accurate, relevant, up-to-date, complete and not misleading; and
- (b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

#### **Response: Accept**

The Government agrees that agencies and organisations should, if an individual requests personal information to be corrected, take reasonable steps to correct personal information so that, with reference to a purpose for which the information is held, it is accurate, relevant, up-to-date, complete and not misleading.

Agencies and organisations should also take reasonable steps to correct information that they become aware of as being incorrect other than through an individual seeking access (for example, when notified of a correction to personal information by another party).

It would be necessary for the Office of the Privacy Commissioner to publish guidance on the application of this principle. As has been noted in response to recommendation 29-9, the Office of the Privacy Commissioner could provide additional guidance on the manner in which personal information can be corrected.

#### ***Requirement to notify third parties of corrections***

Agencies and organisations should, where they have corrected personal information, notify other entities to which the personal information has already been disclosed by the agency or

organisation, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

As this requirement would be based on taking 'reasonable steps', then a range of factors would be relevant to considering what steps, if any, to take to notify third parties of a correction made. Such factors could include the materiality of the correction and the potential for adverse consequences to the individual if incorrect information is used or disclosed.

An agency or organisation's Privacy Policy could outline information relevant to notifying third parties of corrections as part of outlining the steps individuals may take to access and correct personal information held about them by the agency or organisation, as would be required by the 'openness' principle (see recommendation 24-1).

Guidance from the Office of the Privacy Commissioner would be helpful to assist agencies and organisations in responding to notifications they receive regarding corrections to an individual's personal information.

**Recommendation 29–6** The 'Access and Correction' principle should provide that an agency or organisation must, in the following circumstances, if requested to do so by the individual concerned, take reasonable steps to associate with the record a statement of the correction sought:

- (a) if the agency or organisation that holds personal information is not willing to correct personal information in accordance with a request by the individual concerned; and
- (b) where the personal information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.

#### **Response: Accept in principle**

Agencies and organisations should be required to take reasonable steps to 'associate' with a disputed record of personal information a statement of the correction sought by the individual.

This statement should be associated in such a way that it is apparent to subsequent users of the disputed information.

The Government accepts this recommendation in principle, as it may not be necessary to include paragraph (b) in the proposed 'access and correction' principle.

#### ***Amend rights of amendment and annotation in the Freedom of Information Act 1982***

In addition to recommendations 29-5 and 29-6, which would amend the rights of correction and annotation of personal information held by agencies, the Government proposes that the provisions of Part V of the FOI Act that set out rights of amendment and annotation should be made consistent with the rights under the Privacy Act.

The ALRC and Administrative Review Council, in its joint report *Open Government: A Review of the Federal Freedom of Information Act 1982*, ALRC 77 (1995), made a series of recommendations in relation to the rights of amendment and annotation of personal information under the FOI Act.

Through the proposed 'access and correction' principle applying to agencies, a number of these recommendations would, in effect, be implemented in relation to correction of personal

information held by agencies.

The Government proposes to implement recommendations 77 to 80 of ALRC 77 to amend the FOI and Privacy Acts to address these issues of consistency of correction and annotation rights.

**Recommendation 29–7** The ‘Access and Correction’ principle should provide that an agency or organisation must:

- (a) respond within a reasonable period of time to a request from an individual for access to his or her personal information held by the agency or organisation; and
- (b) provide access in the manner requested by the individual, where reasonable and practicable.

**Response: Accept with amendment**

The Government agrees that the ‘access and correction’ principle should include general requirements in relation to the procedural matters outlined in the recommendation.

Consistent with principles-based regulation, these requirements should not be overly prescriptive and should be able to apply across the diverse range of agencies and organisations covered by the Privacy Act.

Guidance from the Office of the Privacy Commissioner on procedural matters in responding to requests for access and correction will be important (see recommendation 29-9).

The Government notes that the recommendation does not refer to the additional procedural matter of charging fees for access.

Consistent with the ALRC’s views expressed in the report and existing National Privacy Principle 6.4, the Government agrees that the principle should provide that, where an organisation imposes a charge for providing access to personal information, the charge must not be excessive and must not apply to lodging a request for access.

This provision should not apply to agencies. Consistent with the Government’s commitment to allow individuals to access their own personal information free of charge under the *Freedom of Information Act 1982* (FOI Act), which is being progressed in the Government’s reform of the FOI Act, agencies should not be permitted to charge an individual for access to his or her own personal information under the Privacy Act.

For the sake of clarity, the Government notes that agencies and organisations should not be able to charge fees for corrections and annotations of personal information, consistent with the existing approach under the Privacy Act and FOI Act.

**Recommendation 29–8** The ‘Access and Correction’ principle should provide that where an agency or organisation denies a request for access, or refuses to correct personal information, it must provide the individual with:

- (a) reasons for the denial of access or refusal to correct personal information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the personal information; and
- (b) notice of potential avenues for complaint.

**Response: Accept with amendment**

The Government agrees it is an important element of procedural fairness for individuals to be provided with the reasons for an adverse decision. Further, a requirement to provide reasons can encourage greater care in decision-making by agencies and organisations and enhance the ability for individuals to assess whether a decision could be challenged through the complaints process.

The principle should explicitly provide for situations where providing reasons would undermine the reasons for denying the request for access or correction (such as where specifying the exception being relied on would prejudice an investigation into unlawful activity).

Additionally the principle should recognise that, where reasons can be provided for an adverse decision, the reasons should specify any relevant exceptions, requirements or authorisations relied on in making the decision.

The ‘access and correction’ principle is to entitle individuals to have access to their personal information, except to the extent an exception applies (organisations) or it is required or authorised to refuse access (agencies) (see recommendation 29-2).

Proper compliance with the principle would require an appropriate exception, requirement or authorisation to have been identified to be able to reach a decision to refuse access. It would therefore not be an additional burden to communicate to the individual the specific exception, requirement or authorisation relied on to the extent that it has already been identified.

It is appropriate that, in giving reasons for an adverse decision, agencies and organisations also provide notice of the potential avenues for complaint available to an individual. The Government notes that agencies and organisations would be required to:

- outline in their Privacy Policy the avenues of complaint available to individuals in relation to privacy complaints (under the proposed ‘openness’ principle); and
- include in collection notices the fact that avenues of complaint are available, referring to the additional information available in its Privacy Policy (under the proposed ‘notification’ principle).

**Recommendation 29–9** The Office of the Privacy Commissioner should develop and publish guidance on the ‘Access and Correction’ principle, including:

- (a) when personal information is ‘held’ by an agency or organisation;
- (b) the requirement that access to personal information should be provided to the maximum extent possible consistent with relevant exceptions;
- (c) the factors that an agency or organisation should take into account when determining what is a reasonable period of time to respond to a request for access;
- (d) the factors that an agency or organisation should take into account in determining when it would be reasonable and practicable to notify other entities to which it has disclosed personal information of a correction to this information; and
- (e) the interrelationships between access to, and correction of, personal information under the *Privacy Act* and other Commonwealth laws, in particular, those relating to freedom of information.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

As a number of changes to existing access and correction requirements are proposed, the Government agrees with the ALRC that agencies and organisations would benefit from clear guidance on how these changes should be applied. Guidance on the principle, and in particular the matters specified in paragraphs (a) to (e) of the recommendation, will be essential in assisting agencies and organisations to understand their obligations under this principle.

In relation to paragraph (e), the Government notes the proposed establishment of the Office of the Information Commissioner, which will co-locate the existing Privacy Commissioner and new positions of Information Commissioner and Freedom of Information Commissioner. This will provide new possibilities for the coordinated development of government information policy, including in the development of guidance on the interrelationships between different access and correction regimes under the *Privacy Act* and *Freedom of Information Act 1982*.

Additional matters which guidance should address, as foreshadowed by the ALRC at [29.116], are the manner in which personal information can be corrected (such as amending the information, deleting incorrect information or adding to the information), and potential conflicts between the requirements of the principle and other record-keeping obligations, including those under the *Archives Act 1983*.



## 30. Identifiers

**Recommendation 30–1** The model Unified Privacy Principles should contain a principle called ‘Identifiers’ that applies to organisations.

### Response: Accept

Due to the high level of reliability of Government issued identifiers to verify and identify an individual, such identifiers are effective tools for linking personal information. However, they can also be highly privacy intrusive if used inappropriately.

While it is appropriate that agencies can use and disclose identifiers in accordance with their functions to provide a public benefit (subject to appropriate regulation), there must be protections to prevent misuse of such identifiers by the private sector.

The Government agrees that identifiers issued by agencies should be subject to additional regulation with regard to how they may be handled by private sector organisations.

The Government notes that section 7A of the Privacy Act provides that acts of certain agencies are to be treated as the acts of organisations. The policy intent of section 7A is that bodies operating in the commercial sphere should operate on a level playing field. Where agencies are engaged in commercial activities, they should be required to comply with the Privacy Principles just like private sector organisations. A note should accompany the ‘identifiers’ principle that draws attention to the role of section 7A.

**Recommendation 30–2** The ‘Identifiers’ principle should include an exception for the adoption, use or disclosure by prescribed organisations of prescribed identifiers in prescribed circumstances. These should be set out in regulations made:

- (a) in accordance with the regulation-making mechanism set out in the *Privacy Act*; and
- (b) when the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

### Response: Accept in principle

The Government acknowledges that there are circumstances where the use and disclosure of a government identifier by an organisation will allow them to provide a strong benefit to an individual. A clear example of this is where an organisation uses and discloses an identifier for the purposes of verifying whether an individual should be entitled to a concession. This provides significant benefit to the individual and ensures organisations are providing benefits only to legitimate claimants.

The Government therefore agrees that there should be a mechanism which provides the flexibility to allow prescribed identifiers to be adopted, used or disclosed by organisations in prescribed circumstances. The Government will ensure that the regulation power provides sufficient scope to allow organisations to interact with agency identifiers where there is a clear benefit to the individual.

The Government intends to work with the Office of Parliamentary Counsel to enhance the value of the regulation making power. The current power has resulted in a procedural mechanism which does not require meaningful consultation between Ministers and the Office of the Privacy Commissioner.

Current regulation processes require individual organisations to be prescribed and this has resulted in significant delays in organisations providing much needed concessional services to individuals. The Government intends to extend the regulation power to allow a class of organisations to be prescribed. It is intended that the Government would still be required to articulate the types of organisations that can interact with agency identifiers to provide services which are for the public benefit but that this is done in a meaningful way.

The 'identifiers' principle will also include exceptions that reflect those provided in existing National Privacy Principle 7 (with amendments as proposed in the 'use and disclosure' principle). These exceptions will continue to ensure that identifiers can be used and disclosed in accordance with law, to prevent a serious threat to an individual's life, health or safety and to assist in law enforcement investigations.

**Recommendation 30–3** The 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

- (a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or
- (b) is determined to be an identifier by the Privacy Commissioner.

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

**Response: Not accept**

The Government does not believe that it is necessary for the 'identifiers' principle to apply to biometric information that is collected for the purpose of automated biometric identification or verification. The collection of such information by organisations will not result in the privacy risks that the 'identifiers' principle is intended to address, such as the risk of an identifier becoming widely held and applied to facilitate extensive data-matching or data-linking.

However, to future-proof the types of identifiers regulated by the principle, the Minister responsible for the Privacy Act (rather than the Privacy Commissioner) will be able to determine what a government identifier is for the purposes of the Act. This will be similar to the Minister's ability to prescribe lawful activities of organisations in relation to identifiers.

'Identifier' will be defined inclusively to mean a number or symbol that uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations or is determined to be an identifier by the Minister but does not include an Australian Business Number.

**Recommendation 30–4** The 'Identifiers' principle should contain a note stating that a determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth).

**Response: Accept in principle**

The Government agrees that the Minister's ability to prescribe identifiers, as outlined in recommendation 30-3, should be a legislative instrument. However, specific matters of

drafting will be the responsibility of the Office of Parliamentary Counsel.

**Recommendation 30–5** The ‘Identifiers’ principle should regulate the adoption, use and disclosure by organisations of identifiers that are assigned by state and territory agencies.

**Response: Accept in principle**

The Government agrees that the unauthorised adoption, use and disclosure of state and territory identifiers carries the same risks to an individual’s privacy as can occur with Commonwealth identifiers.

However, the Government also acknowledges the importance that state and territory identifiers play in allowing organisations to verify an individual’s identity in order to prevent fraudulent or misleading transactions. The ALRC acknowledged in its report that the ‘identifier’ principle was not intended to restrict organisations using an identifier to verify an identity where it was necessary to their functions. The Government notes the ALRC’s drafting in the model ‘identifier’ principle does not adequately reflect this policy intent.

The Government will ensure that the ‘identifier’ principle is drafted to reflect that the principle is not intended to restrict identifiers being collected, used or disclosed for the sole purpose of verifying the identity of an individual where it is relevant and necessary to the organisation’s functions. This would mean that the identifier could not be used for related purposes such as data-matching and could only be used or disclosed for verification purposes which are objectively considered to be necessary to the organisation’s business practices.

The Government would encourage the Privacy Commissioner to develop guidance on the appropriate use and disclosure of identifiers for verification purposes.

**Recommendation 30–6** Before the introduction by an agency of any multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should conduct a Privacy Impact Assessment.

**Response: Accept in principle**

The Government notes the importance of understanding the effect policies will have on the privacy of individuals and recognises that Privacy Impact Assessments are a valuable tool to assist in this process (as evidenced in the acceptance of recommendation 47-4).

The Government acknowledges that the creation of any multi-purpose identifier requires strong consideration of what privacy protections are necessary to ensure individuals’ information is used appropriately.

**Recommendation 30–7** The Office of the Privacy Commissioner, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the Tax File Number Guidelines issued under s 17 of the *Privacy Act*.

**Response: Accept**

The Government agrees that it would be timely and appropriate for the Office of the Privacy Commissioner to conduct a review of the Tax File Number Guidelines issued under section 17 of the Privacy Act, though it is noted that this is a decision for the Privacy Commissioner.

## 31. Cross-border Data Flows

**Recommendation 31–1** (a) The *Privacy Act* should be amended to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency.

(b) The model Unified Privacy Principles should contain a principle called ‘Cross-border Data Flows’ that applies to agencies and organisations.

### Response: Accept

The Government agrees with the conclusions of the ALRC on the desirability of extending cross-border protections for personal information to the acts and practices of agencies.

**Recommendation 31–2** The ‘Cross-border Data Flows’ principle should provide that, if an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia or an external territory, the agency or organisation remains accountable for that personal information, unless the:

- (a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model Unified Privacy Principles;
- (b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual’s personal information once transferred; or
- (c) agency or organisation is required or authorised by or under law to transfer the personal information.

### Response: Accept with amendment

The Government accepts this recommendation with modifications. The Government accepts the general principle that an agency or organisation should remain accountable for personal information that is transferred outside Australia. The Government accepts that there should be a limited number of exceptions to this principle whereby the agency or organisation will no longer be accountable. The Government accepts the exceptions set out in paragraphs (b) and (c) of the recommendation.

The Government considers the exception recommended by the ALRC in paragraph (a) should be modified. The exception should only apply in situations where the recipient of the personal information who is outside Australia is subject to obligations to uphold privacy protections substantially similar to the Privacy Principles and where there are accessible mechanisms for individuals to be able to take effective action to have the privacy protections enforced. The Government recognises that the application of laws or binding schemes may satisfy both these requirements. However, the Government does not consider that the application of contractual obligations on the recipient of the information provides an individual with any rights to take action under the contract. While contracts are important mechanisms for agencies and organisations to impose obligations upon recipients, they should not provide an exception from the general accountability obligations.

Consistent with this approach, the Government considers that any law or binding scheme must have effective enforcement mechanisms which can be used to protect the personal

information of Australians transferred into the jurisdiction to which the law or binding scheme applies. The Government notes that effective enforcement mechanisms may be expressly included in the law or binding scheme or may take effect through the operation of cross-border enforcement arrangements between the Office of the Privacy Commissioner and an appropriate regulatory authority in the foreign jurisdiction.

In addition, the Government considers that the following exceptions to the general principle of remaining accountable should also apply:

- (d) the agency or organisation reasonably believes that the disclosure is necessary to lessen or prevent a serious threat to:
  - (i) an individual's life, health or safety; or
  - (ii) public health or public safety;where in the circumstances, it is unreasonable or impracticable to seek the individual's consent;
- (e) the agency or organisation has reason to suspect that unlawful activity or serious misconduct has been, is being or may be engaged in, and the disclosure of the personal information is a necessary part of its own investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- (f) the agency or organisation reasonably believes that the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law.

**Recommendation 31–3** The *Privacy Act* should be amended to provide that 'accountable', for the purposes of the 'Cross-border Data Flows' principle, means that where an agency or organisation transfers personal information to a recipient (other than the agency, organisation or the individual) that is outside Australia or an external territory:

- (a) the recipient does an act or engages in a practice outside Australia or an external territory that would have been an interference with the privacy of the individual if done or engaged in within Australia or an external territory; and
- (b) the act or practice is an interference with the privacy of the individual, and will be taken to have been an act or practice of the agency or organisation.

**Response: Accept**

It will be important for the term 'accountable' to be defined so that the scope of the principle is clear to agencies and organisations.

**Recommendation 31–4** A note should be inserted after the:

- (a) 'Use and Disclosure' principle, cross-referencing to the 'Cross-border Data Flows' principle; and
- (b) 'Cross-border Data Flows' principle, cross-referencing to the 'Use and Disclosure' principle.

**Response: Accept**

This and other appropriate notes identifying cross-references will be considered in the drafting process.

**Recommendation 31–5** Section 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia or an external territory, the transfer will be subject to the 'Cross-border Data Flows' principle.

**Response: Accept**

The Government accepts this is an appropriate clarification.

**Recommendation 31–6** The Australian Government should develop and publish a list of laws and binding schemes in force outside Australia that effectively uphold principles for the fair handling of personal information that are substantially similar to the model Unified Privacy Principles.

**Response: Accept**

A Government list of laws and binding schemes outside Australia which uphold Privacy Principles that are substantially similar to the Privacy Principles will provide guidance to agencies and organisations. Agencies and organisations will be able to use the list to assist them in forming a reasonable belief that, in the circumstances of their particular cross-border transfer of personal information, the recipient of the information will be accountable. This will include considering all relevant matters, such as whether the particular law or binding scheme in operation outside Australia provides exemptions or other limitations that would apply to the recipient.

**Recommendation 31–7** The Office of the Privacy Commissioner should develop and publish guidance on the ‘Cross-border Data Flows’ principle, including guidance on:

- (a) circumstances in which personal information may become available to a foreign government;
- (b) outsourcing government services to organisations outside Australia;
- (c) the issues that should be addressed as part of a contractual agreement with an overseas recipient of personal information;
- (d) what constitutes a ‘reasonable belief’;
- (e) consent to cross-border data flows, including information for individuals on the consequences of providing consent;
- (f) the establishment by agencies of administrative arrangements, memorandums of understanding or protocols with foreign governments, with respect to appropriate handling practices for personal information in overseas jurisdictions where privacy protections are not substantially similar to the model Unified Privacy Principles (for example, where the transfer is required or authorised by or under law); and
- (g) examples of circumstances which do, and do not, constitute a transfer for the purposes of the ‘Cross-border Data Flows’ principle.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

Guidance on this principle will be very important for organisations and agencies which undertake cross-border transfers of personal information. For example, providing advice on circumstances which do, and do not, constitute a transfer for the purposes of the principle will help to clarify that the principle is intended to apply to personal information accessed or stored outside Australia, but not to any personal information that may be routed or temporarily stored outside Australia. Similarly, guidance for agencies on the establishment of administrative arrangements or other understandings will be particularly important for the effective implementation of this principle.



**Recommendation 31–8** The Privacy Policy of an agency or organisation, referred to in the ‘Openness’ principle, should set out whether personal information may be transferred outside Australia and the countries to which such information is likely to be transferred.

**Response: Accept**

Guidance from the Office of the Privacy Commissioner on the meaning of ‘transfer’ will assist agencies and organisations in determining the extent of their notification requirements.

As stated in relation to recommendation 23-2, the Government notes community concern regarding the flow of personal information overseas. Accordingly, agencies and organisations should also take such steps, if any, as are reasonable in the circumstances to notify individuals if their personal information is reasonably likely to be transferred overseas and to where it may be transferred.

This requirement would be expressly stated in the ‘notification’ principle. The requirement would be qualified by the ‘reasonable steps’ test. For example, an agency or organisation would not need to include this information in a collection notice if it did not reasonably know at the time of collection whether information would be transferred overseas.

Further, it would not be reasonable to provide specific information if the organisation or agency does not reasonably know to which specific jurisdiction personal information may be transferred.

## 44. New Exemptions or Exceptions (Confidential Alternative Dispute Resolution Processes)

**Recommendation 44–1** The *Privacy Act* should be amended to provide an exception to the:

- (a) ‘Collection’ principle to authorise the collection of sensitive information, and
- (b) ‘Use and Disclosure’ principle to authorise the use and disclosure of personal information,

where the collection, use or disclosure by an agency or organisation is necessary for the purpose of a confidential alternative dispute resolution process.

### **Response: Accept**

In chapter 44 of its report, the ALRC discussed whether alternative dispute resolution (ADR) schemes should be subject to a general exemption from the Privacy Act. The ALRC decided that ADR schemes should not be subject to an exemption, though the ‘collection’ and ‘use and disclosure’ principles should each contain provision for the exchange of information for the purposes of confidential ADR schemes.

The Government has undertaken to consider matters relating to exemptions from the Privacy Act in the second stage of its response to the ALRC’s recommendations. However, it is appropriate that the ALRC’s recommendations for confidential ADR schemes be considered in this first stage, as they will affect the content of the relevant proposed principles.

The Government accepts that the ‘collection’ and ‘use and disclosure’ principles should include exceptions for confidential ADR schemes.

**Recommendation 44–2** The Office of the Privacy Commissioner, in consultation with the National Alternative Dispute Resolution Advisory Council, should develop and publish guidance on what constitutes a confidential alternative dispute resolution process for the purposes of the *Privacy Act*.

### **Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

## PART F – OFFICE OF THE PRIVACY COMMISSIONER

### 46. Structure of the Office of the Privacy Commissioner

**Recommendation 46–1** The *Privacy Act* should be amended to change the name of the ‘Office of the Privacy Commissioner’ to the ‘Australian Privacy Commission’.

**Response: Not accept**

The Government is committed to establishing the Office of the Information Commissioner which will incorporate the functions of the current Office of the Privacy Commissioner. The Privacy Commissioner will be a statutory officer within this new Office which is proposed to be established under the Information Commissioner Bill 2009.

**Recommendation 46–2** The *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. The Act should provide that, subject to the oversight of the Privacy Commissioner, the Deputy Commissioners may exercise all the powers, duties and functions of the Privacy Commissioner under the Act or any other enactment.

**Response: Not accept**

Statutory appointment of Deputy Commissioners does not align with the Office of the Information Commissioner model as proposed in the Information Commissioner Bill 2009. Statutory appointment of Deputy Commissioners will be unnecessary due to the model of three Commissioners proposed in that Bill.

**Recommendation 46–3** The *Privacy Act* should be amended to provide that the Privacy Commissioner must have regard to the objects of the Act, as set out in Recommendation 5-4, in the performance of his or her functions and the exercise of his or her powers.

**Response: Accept**

The Government agrees that consistent with implementing an objects clause (as agreed to in recommendation 5-4), it is important that the Privacy Commissioner have regard to these objects in undertaking functions and exercising his or her powers. This will ensure that matters that the Privacy Commissioner has regard to in the administration of the Privacy Act are in line with the objects by which the community interprets and applies the Act.

**Recommendation 46–4** The *Privacy Act* should be amended to make the following changes in relation to the Privacy Advisory Committee:

- (a) expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven;
- (b) require the appointment of a person who has extensive experience in health privacy; and
- (c) replace ‘electronic data-processing’ in s 82(7)(c) with ‘information and communication technologies’.

**Response: Accept with amendment**

The Government agrees with the ALRC’s recommendations to require the appointment of a person with extensive health privacy experience to the Privacy Advisory Committee (PAC) and to update section 82(7)(c).

The Government also considers that the membership criteria should be amended to separate the criteria in section 82(7)(a) to require the appointment of both a high level person in industry or commerce and a high level person in public administration or government. This will ensure that the Government has the discretion to appoint such members separately in order to fairly represent private and public sector interests. The membership of the PAC will be expanded to no more than eight members to provide the Government with the discretion to appoint a diverse cross-section of the community on the PAC.

The Government will continue to ensure that appointments made to the Committee adequately balance business, community and government interests.

**Recommendation 46–5** The *Privacy Act* should be amended to empower the Privacy Commissioner to establish expert panels, at his or her discretion, to advise the Privacy Commissioner.

**Response: Accept**

A broad, discretionary power to establish either temporary or permanent panels will provide the Privacy Commissioner with an explicit tool for engaging experts to assist with the Commissioner’s functions. Unlike the powers to establish the Privacy Advisory Committee, this power will not be prescriptive and instead will provide a broad power to allow the Commissioner to establish advisory committees to assist in undertaking his or her functions.

## 47. Powers of the Office of the Privacy Commissioner

**Recommendation 47–1** The *Privacy Act* should be amended to delete the word ‘computer’ from s 27(1)(c).

### Response: Accept

The removal of ‘computer’ from the Privacy Commissioner’s oversight functions will ensure that the research and monitoring role remains technology-neutral. This will ensure that there are no impediments to the Commissioner’s ability to produce guidelines in relation to new and emerging technologies in line with the ALRC’s recommendations in Part B.

**Recommendation 47–2** The *Privacy Act* should be amended to reflect that, where guidelines issued or approved by the Privacy Commissioner are binding, they should be renamed ‘rules’. For example, the following should be renamed to reflect that a breach of the rules is an interference with privacy under s 13 of the *Privacy Act*:

- (a) Tax File Number Guidelines issued under s 17 of the *Privacy Act* should be renamed the *Tax File Number Rules*;
- (b) Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs (issued under s 135AA of the *National Health Act 1953* (Cth)) should be renamed the *Privacy Rules for the Medicare Benefits and Pharmaceutical Benefits Programs*;
- (c) Data-Matching Program (Assistance and Tax) Guidelines (issued under s 12 of the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth)) should be renamed the *Data-Matching Program (Assistance and Tax) Rules*; and
- (d) Guidelines on the Disclosure of Genetic Information to a Patient’s Genetic Relative should be renamed the *Rules for the Disclosure of Genetic Information to a Patient’s Genetic Relative*.

### Response: Accept

A distinction between what are binding ‘rules’ and non-binding ‘guidelines’ as issued by the Privacy Commissioner will provide clarity as to the status of different guidance under the *Privacy Act*.

**Recommendation 47–3** Subject to the implementation of Recommendation 24–1, requiring agencies to develop and publish Privacy Policies, the *Privacy Act* should be amended to remove the requirement in s 27(1)(g) to maintain and publish the Personal Information Digest.

### Response: Accept

The Government considers that the revised ‘openness’ principle will place a strong onus on agencies to publicly outline how they collect, hold, use and disclose personal information. Agencies will be required to ensure that their privacy policies are updated to reflect changes in information handling practices and this will fulfil the role of the Personal Information

Digest.

The Government notes that the 'openness' principle outlines the minimum amount of information that should be included in a privacy policy and that agencies would also be expected to provide any other information deemed necessary to express their practices, including that which is currently outlined in Information Privacy Principle 5.3.

**Recommendation 47–4** The *Privacy Act* should be amended to empower the Privacy Commissioner to:

- (a) direct an agency to provide to the Privacy Commissioner a Privacy Impact Assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and
- (b) report to the ministers responsible for the agency and for administering the *Privacy Act* on the agency's failure to comply with such a direction.

**Response: Accept**

The Government agrees that a Privacy Impact Assessment (PIA) is a best practice tool which can provide a valuable evaluation of how a project or policy may impact on an individual's privacy and possible solutions to address those issues. In line with the principles-based approach of the Privacy Act, PIAs allow agencies and organisations to consider how to best put the Privacy Principles into practice and it is appropriate that PIAs are voluntary in nature.

The Government supports this recommendation. It is important that the Privacy Commissioner have the discretion to direct an agency to undertake a PIA where it is considered that it is crucial to ensuring that a policy or project is appropriately balanced against an individual's right to privacy. This is in line with the Privacy Commissioner's role in enforcing the requirements of the Privacy Act and with the strong need to ensure that Government policy is appropriately balanced against privacy requirements.

This discretionary power is not intended to reduce the voluntary nature of PIAs nor mean that PIAs should only be conducted where there is a direction from the Privacy Commissioner. It will still be necessary for agencies to determine when developing a policy whether it will impact on privacy and whether a PIA is required. This is intrinsically linked with the agency's obligation to comply with the Privacy Principles.

**Recommendation 47–5** The Office of the Privacy Commissioner should develop and publish Privacy Impact Assessment Guidelines tailored to the needs of organisations. A review should be undertaken in five years from the commencement of the amended *Privacy Act* to assess whether the power in Recommendation 47–4 should be extended to include organisations.

**Response: Accept**

The Government agrees that voluntary guidelines would provide organisations with a tool to assist them in making an assessment about when a Privacy Impact Assessment (PIA) should be undertaken. The Government notes that PIAs are a valuable tool to assist an organisation to comply with its responsibilities under the Privacy Act but agrees with the

ALRC that a similar power to that recommended in 47-4 for agencies should not be available in relation to organisations at this stage.

The Government encourages the development and publication of tailored guidance on PIAs for organisations by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner. Subject to the development of tailored guidelines, the Government agrees that it would be appropriate in the future to consider whether recommendation 47-4 should be extended to organisations.

**Recommendation 47–6** The *Privacy Act* should be amended to empower the Privacy Commissioner to conduct ‘Privacy Performance Assessments’ of the records of personal information maintained by organisations for the purpose of ascertaining whether the records are maintained according to the model Unified Privacy Principles, privacy regulations, rules and any privacy code that binds the organisation.

**Response: Accept**

An important role of the Privacy Commissioner is to assist organisations to comply with the Privacy Act through education and guidance. An ability to conduct Privacy Performance Assessments (PPA) would allow the Privacy Commissioner to provide one-on-one guidance for organisations without needing to resort to mandatory enforcement action. This is in line with the overall approach of the Privacy Act to encourage organisations to proactively respond to privacy regulation as a good business practice rather than enforcing compliance through sanctions.

The Government notes that the power to conduct PPAs will be distinguished from the Privacy Commissioner’s ability to conduct own motion investigations. Unlike the own motion investigation power, the PPA power is not intended to be a means by which the Office of the Privacy Commissioner (OPC) can investigate and impose sanctions for contraventions of the Privacy Act.

The Government does not consider it necessary to provide legislative criteria for when a PPA could or should be conducted but considers that it would be in line with OPC’s current approach to auditing agencies. OPC will retain the flexibility and discretion to conduct PPAs as necessary but these are most likely to occur where organisations or agencies are undertaking actions which significantly impact on an individual’s privacy or are undertaking new ways of dealing with personal information which could impact on privacy.

**Recommendation 47–7** The Office of the Privacy Commissioner should publish and maintain on its website a list of all the Privacy Commissioner’s functions, including those functions that arise under other legislation.

**Response: Accept**

While the Government attempts to ensure that the Privacy Commissioner’s functions are clearly listed in the Privacy Act, it is often impractical for the Act to be amended each time the Privacy Commissioner is given a new function under other legislation.

The Government strongly encourages the Office of the Privacy Commissioner to clearly outline all its functions on its website. This will ensure that a complete list of the Office’s

functions can be obtained from one source.

**Recommendation 47–8** The *Privacy Act* should be amended to empower the Privacy Commissioner to refuse to accept an application for a Public Interest Determination where the Privacy Commissioner is satisfied that the application is frivolous, vexatious or misconceived.

**Response: Accept in principle**

The Government agrees with the ALRC's recommendation to set a high threshold test which the Privacy Commissioner must be satisfied of before dismissing a Public Interest Determination (PID) application outright.

To ensure consistency with similar provisions in the Freedom of Information Amendment Bill 2009 refusal of a PID application will also be allowed where the application is 'lacking in substance or not made in good faith'.

The Government encourages all future applicants to discuss their applications with the Office of the Privacy Commissioner, prior to submission and in accordance with the Office's *Public Interest Determination Procedure Guidelines 2002*, to ensure that they would not fall within the proposed dismissal criteria.



## 48. Privacy Codes

**Recommendation 48–1** Part IIIAA of the *Privacy Act* should be amended to specify that a privacy code:

- (a) approved under Part IIIAA operates in addition to the model Unified Privacy Principles (UPPs) and does not replace those principles; and
- (b) may provide guidance or standards on how any one or more of the model UPPs should be applied, or are to be complied with, by the organisations bound by the code, as long as such guidance or standards contain obligations that, overall, are at least the equivalent of all the obligations set out in those principles.

### **Response: Accept in principle**

The Government agrees that the Privacy Principles should be the base standard for privacy protection and that codes should be developed to provide guidance about how some or all of the principles apply in certain contexts.

The Government notes that it was not the ALRC's intention in paragraph (a) that the protections in the code cannot expand upon or enhance the protections in the Privacy Principles. This means that in some instances a code may 'replace' concepts in the principles to the extent the code adds to the requirements by providing for a more specific or higher standard of privacy protection. For example an organisation would be able to narrow the application of the 'use and disclosure' principle so that personal information could only be used for a primary purpose or the concept of 'reasonable' access in the 'access and correction' principle could be replaced with a prescribed fee for access.

The code power will therefore allow organisations to offer protections in excess of those offered by the privacy principle but only to the extent that these protections do not derogate from the principles.

#### ***Binding codes***

In addition to recommendation 48-1, the Privacy Commissioner should be given the power to request the development of a privacy code by a defined group of organisations/agencies where the Commissioner considers that the public interest would be served by the development of such a code. The defined group of organisations/agencies would be either an industry sector or a group of organisations/agencies who engage in a prescribed practice (such as using certain tools or technologies). The code would be developed by the organisations/agencies in line with recommendation 48-1 and would be approved by the Commissioner subject to the requirements of Part IIIAA. The code would be mandatory for all those organisations/agencies as defined in the code.

Where an adequate code is not developed or approved, the Privacy Commissioner would be empowered to develop and impose a privacy code that mandatorily applies to a defined group of organisations/agencies. This power would be subject to a requirement to undertake consultation with relevant stakeholders similar to that currently required for Public Interest Determinations.

This would result in a three tiered model for code development: codes voluntarily developed by organisations; mandatory codes developed at the request of the Privacy Commissioner; and where such a request is not complied with, a mandatory code developed by the Privacy Commissioner.

This model is based on Part 6 of the *Telecommunications Act 1997* (Cth) and the mandatory codes will have the same application as recommended in recommendation 48-1 and as currently applies in Part IIIAA of the *Privacy Act*. The codes would be distinguished from the

telecommunications model in that they would not create standards which would attempt to derogate from the Privacy Principles but would provide more specific standards for sector groups or for specific practices. These codes may go beyond the application of the Privacy Principles to the extent that they do not derogate from the principles.

A breach of a binding code would be an interference with privacy under section 13A of the Privacy Act and would be subject to the usual enforcement mechanisms available for an interference with privacy.

## 49. Investigation and Resolution of Privacy Complaints

**Recommendation 49–1** The *Privacy Act* should be amended to provide that, in addition to existing powers not to investigate, the Privacy Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made, or which the Commissioner has accepted under s 40(1B), if the Commissioner is satisfied that:

- (a) the complainant has withdrawn the complaint;
- (b) the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint; or
- (c) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.

### Response: Accept

Implementation of this recommendation will allow the Office of the Privacy Commissioner to more effectively devote its resources to efficiently deal with complaints that warrant investigation.

The Government understands the concerns raised about the possible breadth of paragraph (c) of recommendation 49-1 and notes that the Office will be:

- (i) subject to the principles of administrative law (including procedural fairness) when making a decision under paragraph (c);
- (ii) expected to outline in its annual report the extent to which paragraph (c) is relied upon; and
- (iii) encouraged to provide guidance on what matters it would decline to investigate in accordance with paragraph (c).

**Recommendation 49–2** The *Privacy Act* should be amended to empower the Privacy Commissioner to decline to investigate a complaint where:

- (a) the complaint is being handled by an external dispute resolution scheme recognised by the Privacy Commissioner; or
- (b) the Privacy Commissioner considers that the complaint would be more suitably handled by an external dispute resolution scheme recognised by the Privacy Commissioner, and should be referred to that scheme.

### Response: Accept

The Government agrees that it is appropriate that the Privacy Commissioner should have the discretion to allow complaints to be dealt with by particular external dispute resolution (EDR) schemes which the Commissioner deems can effectively deal with complaints under the Privacy Act. These schemes would generally be those that have a mandate for dealing with privacy issues and have mechanisms in place which provide adequate dispute resolution processes and suitable remedies.

In order to assist in accountability and transparency, the Privacy Commissioner is encouraged to publish the names of the schemes it recognises and where appropriate, develop mechanisms with EDR schemes for reporting on outcomes from privacy disputes.

In line with recommendation 49-8, it would also be expected that the Office of the Privacy Commissioner will publish its procedures for transferring disputes to EDR schemes.

**Recommendation 49–3** The *Privacy Act* should be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers in relation to complaint handling conferred on the Commissioner by the Act.

**Response: Not accept**

The Government does not consider that this recommendation would increase the efficiency or effectiveness of the Office of the Privacy Commissioner's investigations or dispute resolution processes. Instead, any delegation of the Privacy Commissioner's powers would require strong measures to be taken to ensure consistency of decisions between the Office and other bodies, including through the development of guidelines and training.

In addition, the Government is not aware of any concerns raised by complainants or respondents to privacy disputes regarding the ability of the Privacy Commissioner to manage disputes outside those cities where the Privacy Commissioner has a physical presence.

Further, the Government notes that continuing advances in communications technologies, which enable the Privacy Commissioner to appropriately handle complaints where the parties to the complaint are located in states and territories where the Privacy Commissioner does not have a physical presence, further undermines the need for this additional power.

**Recommendation 49–4** The *Privacy Act* should be amended to clarify the Privacy Commissioner's functions in relation to complaint handling and the process to be followed when a complaint is received.

**Response: Accept**

A concise summary of the complaint handling functions and processes of the Privacy Commissioner will provide a clear indication to parties to a dispute how complaints are expected to be dealt with under the Privacy Act.

**Recommendation 49–5** The *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should give effect to the following:

- (a) If, at any stage after accepting the complaint, the Commissioner considers it reasonably possible that the complaint may be conciliated successfully, he or she must make reasonable attempts to conciliate the complaint.
- (b) Where, in the opinion of the Commissioner, reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by

determination.

- (c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.
- (d) Subparagraph (c) does not apply where the communication was made in furtherance of the commission of a fraud or an offence, or in the commission of an act that would render a person liable to a civil penalty.

**Response: Accept with amendment**

Conciliation is a fundamental part of dispute resolution under the Privacy Act and it is important that the conciliation process is clearly set out under the Act. This will provide much needed clarification for complainants and respondents about the role conciliation plays in resolving disputes under the Act and the powers of the Privacy Commissioner to give effect to conciliation.

The Government agrees with the ALRC's recommendations in paragraphs (a), (c) and (d). However it does not support the recommendation in paragraph (b) which would allow parties to a dispute to compel the Privacy Commissioner to make a determination where conciliation fails. This recommendation would fetter the Commissioner's discretion to determine the most effective way to resolve a complaint and could undermine the incentives for parties to engage actively in conciliation.

Where the Privacy Commissioner deems that conciliation has failed, in place of the requirement in paragraph (b), the Commissioner must then decide whether to decline the complaint in line with its amended powers under section 41, investigate the complaint or investigate it further, or resolve the complaint by determination. Where the Privacy Commissioner decides not to investigate or further investigate the complaint and any parties to the complaint are not satisfied with this decision, they will have the ability to make an application directly to the Federal Court alleging interference with their privacy.

The Government encourages the making of determinations by the Privacy Commissioner in appropriate instances, noting that the making of such determinations is a matter for the Privacy Commissioner.

**Recommendation 49–6** The *Privacy Act* should be amended to empower the Privacy Commissioner, in a determination, to prescribe the steps that an agency or respondent must take to ensure compliance with the Act.

**Response: Accept in principle**

It is the Privacy Commissioner's role to assist agencies and organisations to comply with the Privacy Act. It is appropriate that where an agency or organisation is found to have interfered with privacy under the Act, the Commissioner can outline steps which would aid compliance.

The Government notes that the steps which the Commissioner can declare an agency or organisation to take will be those that are reasonable and appropriate in the circumstances.

**Recommendation 49–7** The *Privacy Act* should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner.

**Response: Accept in principle**

The Government understands that enhanced review of determinations made by the Privacy Commissioner would assist in promoting transparency and accountability in the Commissioner's decisions and is consistent with the role of the Administrative Appeals Tribunal (AAT) in reviewing a Commonwealth officer's decision.

The Government will work to develop an appropriate scheme to promote merits review of determinations made by the Privacy Commissioner which is in line with the proposed operation of the Office of the Information Commissioner and within the framework of AAT review.

**Recommendation 49–8** The Office of the Privacy Commissioner should develop and publish a document setting out its complaint-handling policies and procedures.

**Response: Accept**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

The Government agrees that consolidated guidance on the Office's complaint handling procedures would provide accessible and transparent information about the Office's approach to dealing with complaints and provide a valuable tool for complainants and respondents.

**Recommendation 49–9** The *Privacy Act* should be amended to allow a class member to withdraw from a representative complaint at any time if the class member has not consented to be a class member.

**Response: Accept**

An individual should have the capacity to determine whether they want their complaint to be dealt with as a representative complaint. Where they do not, an individual should have the ability to withdraw and have the opportunity to lodge an individual complaint.

**Recommendation 49–10** The *Privacy Act* should be amended to permit the Privacy Commissioner, in accepting a complaint or determining whether the Commissioner has the power to accept a complaint, to make preliminary inquiries of third parties as well as the respondent. The Privacy Commissioner should be required to inform the complainant that he or she intends to make inquiries of a third party.

**Response: Accept**

The Privacy Commissioner will be given the appropriate authority to obtain relevant facts about a complaint to determine as soon as practicable whether to accept and further investigate a complaint.

The Government notes that this power is only intended to be used where making inquiries with a third party will result in a more timely and efficient investigation by the Commissioner. Where information can be obtained easily from a party to a complaint, the Privacy Commissioner would be expected to do so.

***Preliminary inquiries for Own Motion Investigations***

Section 42 will be amended to allow the Office of the Privacy Commissioner to undertake preliminary investigations prior to conducting a formal own motion investigation. This would provide the Office with the ability to make inquiries to determine whether the matter falls within the jurisdiction of the Privacy Act or not. The Office would not be required to comply with the formal requirements of an investigation until it has finalised its preliminary investigation. This is in line with a similar power provided to the Commonwealth Ombudsman.

Consistent with recommendation 49-10, this would allow the Office to make preliminary investigations of an agency or organisation and of any third parties, including those affected by the action (where information is unable to be efficiently and effectively obtained by the party under investigation).

**Recommendation 49–11** Section 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to a complaint, and any other relevant person, to attend a compulsory conference.

**Response: Accept**

The Government agrees that there is no policy reason why section 46 is limited only to complaints concerning the public sector. This recommendation is in line with the Government's intention to promote consistency in the Privacy Act between the public and private sector.

***Enforcement of investigation powers***

Sections 44 and 46 of the Privacy Act will be amended to allow the Privacy Commissioner to apply to the Federal Court for an order directing a person to comply with a request to produce information/documents or to attend a conference. This will provide the Commissioner with an effective remedy where a person fails to comply with a direction under these sections.

**Recommendation 49–12** The *Privacy Act* should be amended to allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant.

**Response: Accept**

The Government will repeal section 69 in its entirety to allow the Privacy Commissioner to collect information about third parties which is relevant to the investigation of a privacy complaint. This is in line with other similar Commonwealth regulatory bodies that do not have this restriction on their investigation functions.

**Recommendation 49–13** The *Privacy Act* should be amended to provide that the Privacy Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties if the Privacy Commissioner is satisfied that the matter could be determined fairly on the basis of written submissions by the parties.

**Response: Accept**

The Government agrees that it is appropriate to provide the Privacy Commissioner with a discretionary power which will facilitate more efficient handling of determination proceedings. This could lead to greater use of the determination power to resolve complaints.

The requirement of ‘fairness’ will ensure that the Privacy Commissioner considers all the relevant circumstances of the parties in deciding whether a written submission will provide an effective consideration of the parties evidence. The Government notes that it would be valuable for the Commissioner to publicly outline the matters to be considered when deciding whether a determination on the papers is ‘fair’. This could occur as part of the complaint-handing guidelines as proposed in recommendation 49-8.



## 50. Enforcing the Privacy Act

**Recommendation 50–1** The *Privacy Act* should be amended to empower the Privacy Commissioner to:

- (a) issue a notice to comply to an agency or organisation following an own motion investigation, where the Commissioner determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual;
- (b) prescribe in the notice that an agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*; and
- (c) commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.

### **Response: Accept**

The Government agrees that this recommendation recognises the importance of own motion investigations conducted by the Privacy Commissioner and that such investigations should have a similar enforcement regime as provided for complaints under section 52.

An enhanced determination power will provide the Privacy Commissioner with a suitable enforcement remedy for those own motion investigations which cannot be finalised by settlement. It would be expected that in line with current processes, the Privacy Commissioner would continue to seek to settle an own motion investigation via conciliation and only proceed to a determination where a settlement is unable to be facilitated or is inappropriate.

**Recommendation 50–2** The *Privacy Act* should be amended to allow the Privacy Commissioner to seek a civil penalty in the Federal Court or Federal Magistrates Court where there is a serious or repeated interference with the privacy of an individual.

### **Response: Accept in principle**

The application of civil penalties, in appropriate circumstances, will complete the enforcement pyramid within the Privacy Act. It will make sanctions available for serious breaches where other compliance oriented enforcement methods are not sufficient. It will mean that appropriate penalties can be directed at those agencies or organisations that show a blatant disregard to the requirements of the Privacy Act or continually breach the Act.

The Government will determine the appropriate implementation of the proposed civil penalty in line with its policy of clearly articulating when a civil penalty will be applied.

**Recommendation 50–3** The Office of the Privacy Commissioner should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty will be made.

**Response: Accept**

The Government encourages the development and publication of tailored guidance on when the Office of the Privacy Commissioner would pursue a civil penalty, noting that the decision to provide guidance is a matter for the Privacy Commissioner.

The Government notes that in line with recommendation 49-8, it is important for the Office to outline its enforcement priorities and the factors it will consider in determining whether to pursue a civil remedy. This will establish transparency in the Office's procedures and in its decisions in relation to enforcement actions.

**Recommendation 50–4** The *Privacy Act* should be amended to empower the Privacy Commissioner to accept an undertaking that an agency or organisation will take specified action to ensure compliance with a requirement of the *Privacy Act* or other enactment under which the Commissioner has a power or function. Where an agency or organisation breaches such an undertaking, the Privacy Commissioner may apply to the Federal Court for an order directing the agency or organisation to comply, or any other order the court thinks appropriate.

**Response: Accept**

The recommendation aligns closely with the compliance-oriented approach of the Privacy Act as it will allow agencies and organisations to take active responsibility for actions which might otherwise result in a court-based outcome.

## PART G – CREDIT REPORTING PROVISIONS

### 54. Approach to Reform

**Recommendation 54–1** The credit reporting provisions of the *Privacy Act* should be repealed and credit reporting regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles, and regulations under the *Privacy Act*—the new *Privacy (Credit Reporting Information) Regulations*—which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information.

#### **Response: Not accept**

In line with the Government's response to recommendation 5-1, the Government does not agree that it is appropriate to have a general regulation-making power that would allow modification of the Privacy Principles. The Government considers that credit reporting information should continue to be regulated primarily under the Privacy Act, with provision for specific regulations to be made where necessary. For example, it would be appropriate to set out a regulation-making power to set the minimum amount at which defaults can be listed with a credit reporting agency.

However, the Government recognises that Part IIIA of the Privacy Act is overly complex and prescriptive and should be redrafted to provide more user-friendly regulation of credit reporting in accordance with the ALRC's recommendations (where accepted).

Where an ALRC recommendation refers to the *Privacy (Credit Reporting Information) Regulations* and the Government accepts the recommendation's intent, the Government will implement that recommendation in primary legislation (the Privacy Act) unless otherwise stated.

**Recommendation 54–2** The new *Privacy (Credit Reporting Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model Unified Privacy Principles.

#### **Response: Accept**

The Government agrees that, to the extent possible, the Privacy Principles should set out the foundation for protecting credit reporting information. Regulation of credit reporting information in the Privacy Act will only set out further requirements where it is necessary for different or more specific protections to apply.

Relevant organisations will have to comply with both the Privacy Principles and the proposed credit reporting provisions. However, as the credit reporting provisions will only apply where it is necessary to have either greater or lesser privacy protection, it is intended that these provisions would set the new privacy standard for credit reporting. If there is inconsistency between the protections in the principles and the credit reporting provisions, organisations would be expected to comply with the more specific or different standards in the credit reporting provisions.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 54–3** The new *Privacy (Credit Reporting Information) Regulations* should apply only to ‘credit reporting information’, defined for the purposes of the new regulations as personal information that is:

- (a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or
- (b) held by a credit provider; and
  - (i) has been prepared by a credit reporting agency; and
  - (ii) is used, has been used or has the capacity to be used in establishing an individual’s eligibility for credit.

**Response: Accept**

The policy framework for credit reporting regulation should be to protect a subset of personal information which is maintained by credit reporting agencies and disclosed to credit providers for the purpose of assessing an individual’s eligibility for credit. This framework will ensure that any personal information collected, used and disclosed within the credit reporting system will be afforded specific and appropriate protection.

The Government considers that, to the extent personal information, including publicly available information, is maintained by a credit reporting agency in order to determine eligibility for credit, such information will be covered by the specific requirements of the credit reporting provisions rather than the more general Privacy Principles. However, it is acknowledged that where credit reporting agencies collect personal information, including publicly available information, for purposes other than to assist in assessing an individual’s credit risk, then they can undertake these other transactions subject to compliance with the Privacy Principles and other general obligations under the Privacy Act.

By implementing this definition of ‘credit reporting information’ the Government intends to streamline the credit reporting provisions in order to remove redundant definitions such as ‘credit information file’, ‘credit report’ and ‘report’.

Note: In line with the Government’s response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 54–4** The new *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of ‘credit provider’ under which those agencies and organisations that are currently credit providers for the purposes of the *Privacy Act* (whether by operation of s 11B or pursuant to determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.

**Response: Accept**

The current definition ensures that an appropriate class of businesses are considered to be credit providers and the Government will work to ensure that the intent of this definition is not displaced. The Government will seek to consolidate the current definitions in the Privacy Act and the Privacy Commissioner’s determinations in a clear and simple way.

The Government considers that the definition will be able to be drafted in a way which will remove the need for the Privacy Commissioner to define further the parameters of the definition. In order to avoid disjointed regulation around the definition, the Government will

remove the Privacy Commissioner's determination power in relation to the 'credit provider' definition.

**Definition of credit**

The Government agrees with the ALRC's decision not to recommend expanding the definition of credit to include commercial credit. However, in line with the National Consumer Credit Protection Bill 2009 (NCCP Bill), the Government intends to extend the protections of the credit reporting provisions in the Privacy Act to include credit provided to purchase residential investment properties. It is appropriate to ensure that credit transactions that are afforded protection under the NCCP Bill are adequately protected under the credit reporting provisions.

**Definition of credit reporting agency**

The Government agrees with the ALRC's view that the definition of 'credit reporting agency' in the Privacy Act should continue to apply and should be extended to include Commonwealth agencies that carry on a credit reporting business.

The Government proposes to remove the 'dominant purpose' test from the definition of 'credit reporting business' as it is concerned that any relevant business, regardless of whether credit reporting is a large or small component of its activities, should be covered by the credit reporting provisions. This would continue to allow a business to engage in other activities unrelated to credit reporting without being covered by the credit reporting provisions to the extent that the business activity is not being conducted for a credit reporting purpose.

**Extension of the Act to small business credit providers and credit reporting agencies**

Credit providers and credit reporting agencies that are small businesses will be required to comply with the Privacy Act. This will ensure all credit providers and credit reporting agencies are subject both to the Privacy Principles and credit reporting provisions (in line with recommendation 54-2). The Government will respond to the ALRC's recommendation about removing the small business exemption in its second stage response to the ALRC's report. Any amendments to the Privacy Act made prior to the Government's second stage response will make all credit providers and credit reporting agencies subject to the Act.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 54–5** The new *Privacy (Credit Reporting Information) Regulations* should, subject to Recommendation 54–7, exclude the reporting of personal information about foreign credit and the disclosure of credit reporting information to foreign credit providers.

**Response: Accept**

It should be made clear in the credit reporting provisions that credit reporting agencies cannot maintain information about foreign credit and foreign credit providers or disclose credit reporting information to foreign credit providers.

This restriction is necessary as any benefit that would be obtained in creating greater transparency about an individual's credit risk would be outweighed by the inability of the Privacy Commissioner to enforce effectively the credit reporting provisions against foreign entities.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 54–6** The Australian Government should include credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).

**Response: Accept in principle**

The Government understands the close relationship that Australian credit providers and credit reporting agencies have with their New Zealand counterparts along with the trans-Tasman consumer credit interactions that individuals have in both countries. In some instances, independent verification of credit reporting information about an individual's transactions in both countries would assist credit providers to undertake more efficient and effective assessment of an individual's credit risk.

The Government will determine whether consultation with the New Zealand Government to harmonise credit reporting provisions is necessary based on the outcome of the Government's response to recommendation 54-7. Where consultation is necessary, the appropriate forum will be determined jointly by the Australian and New Zealand Governments.

**Recommendation 54–7** The new *Privacy (Credit Reporting Information) Regulations* should empower the Privacy Commissioner to approve the reporting of personal information about foreign credit, and the disclosure of credit reporting information to foreign credit providers, in defined circumstances. The regulations should set out criteria for approval, including the availability of effective enforcement and complaint handling in the foreign jurisdiction.

**Response: Not accept**

The ALRC identified the main motivation for making this recommendation was to allow recognition of the close relationship between the Australian and New Zealand credit reporting market. It did not specifically consider the application of this power to other jurisdictions. Therefore the Government considers that this recommendation should be tailored to allow trans-Tasman use and disclosure of credit reporting information, where necessary and appropriate.

The Government intends that the Privacy Act will be amended to exclude New Zealand, in limited circumstances, from the prohibition in recommendation 54-5. Following consultation with relevant industry and advocate stakeholders along with the Privacy Commissioner and relevant New Zealand authorities, it will be determined in what defined circumstances credit reporting information should be shared across the Tasman.

The Government understands that the main issue is for credit providers in each jurisdiction to be able to access credit reporting information from the other jurisdiction. Even if disclosure in these limited circumstances was permitted, consideration would still need to be given as to how adequate protections could be put in place to ensure that there was no inappropriate secondary use of the information outside the jurisdiction where the information

was originally held. The Government will also need to ensure that there are effective enforcement mechanisms to ensure that misuse can be appropriately rectified.

The Government considers that any further exclusion to the prohibition in recommendation 54-5 would be more appropriately adopted by legislative amendments than by a determination of the Privacy Commissioner. Further exclusions to the prohibition to allow sharing of credit reporting information with other foreign jurisdictions would only be considered where a clear need arises.

**Recommendation 54–8** The Australian Government should, in five years from the commencement of the new *Privacy (Credit Reporting Information) Regulations*, initiate a review of the regulations.

**Response: Accept in principle**

The Government agrees that the effect of the amendments to the Privacy Act to implement its response to the ALRC's credit reporting recommendations should be reviewed within five years of commencement of the comprehensive credit reporting amendments.

**Recommendation 54–9** Credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, should develop a credit reporting code providing detailed guidance within the framework provided by the *Privacy Act* and the new *Privacy (Credit Reporting Information) Regulations*. The credit reporting code should deal with a range of operational matters relevant to compliance.

**Response: Accept with amendment**

The Government agrees that both industry and advocates require flexibility to ensure that operational procedures consistent and compliant with the Privacy Act. Matters identified by the ALRC to be placed in the credit reporting code would be more suitably placed in an industry-developed code rather than the Privacy Act.

The Government notes that it is necessary to have a clear and transparent code of practice, which is agreed to across the credit reporting industry, about how the credit reporting provisions and related issues will operate in practice. The code will ensure consistency across the industry in relation to matters such as access to information, data accuracy and complaint handling.

The Government considers that an industry code should be developed subject to satisfactory consultation requirements between the credit reporting industry, advocates and the Privacy Commissioner. The Privacy Act will broadly outline the matters to be addressed in the code (including those recommended by the ALRC). It is also intended that the code will replace the current Credit Reporting Code of Conduct developed by the Privacy Commissioner, and will address the matters outlined in that Code of Conduct to the extent they do not overlap with requirements in the redrafted Privacy Act.

The code will operate in line with the proposed binding code power as outlined in recommendation 48-1. The code will operate in addition to the credit reporting provisions and should not seek to override or apply lesser standards than are outlined in the Privacy Act. Instead the code would set out how credit reporting agencies and credit providers can

practically apply the credit reporting provisions.

The Privacy Act will require that any code that is developed is to be approved by the Privacy Commissioner. The Government acknowledges that the credit reporting industry will be the main driver behind the code. However, final approval of the code by the Privacy Commissioner will ensure that the code appropriately balances the needs of industry to have efficient and effective credit reporting with the privacy needs of individuals.

Any organisation or agency (including credit providers and credit reporting agencies) that wants to participate in the credit reporting system will be required to be a member of this binding code. This will ensure consistency across the sector.

A breach of the code will be deemed to be a breach of the Privacy Act to the extent that the code provision is interpreting the application of a credit reporting provision in the Act.

The Government notes that industry may wish to outline matters in the code which are outside the jurisdiction of the Privacy Act and that these matters could be addressed through the relevant approval processes as required by the Australian Competition and Consumer Commission.

The Government will consult further with industry and advocates in drafting the appropriate provisions to establish the power to make a binding industry code in the Privacy Act.



## 55. More Comprehensive Credit Reporting

**Recommendation 55–1** The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include the following categories of personal information, in addition to those currently permitted in credit information files under the *Privacy Act*:

- (a) the type of each credit account opened (for example, mortgage, personal loan, credit card);
- (b) the date on which each credit account was opened;
- (c) the current limit of each open credit account; and
- (d) the date on which each credit account was closed.

### Response: Accept

The Government supports the introduction of comprehensive credit reporting, in line with the ALRC's recommendations, subject to sufficient privacy protections being put in place. The Government considers that the introduction of the five 'positive' data sets proposed by the ALRC in recommendations 55-1 and 55-2 will provide credit providers with an enhanced tool to establish an individual's credit worthiness. Greater access to the five data sets as proposed by the ALRC will allow more robust assessment of credit risk, which in turn could lead to lower credit default rates. On balance, comprehensive credit reporting is also likely to improve competition in the credit market, which will result in benefits to both individuals and the credit industry.

The Government understands the strong privacy and consumer credit concerns that arise with the introduction of a comprehensive credit reporting regime. The Government notes that the ALRC has based a number of recommendations for enhanced protection and dispute resolution for credit reporting information on the introduction of comprehensive credit reporting. The Government supports the introduction of effective privacy protections to ensure that the five data sets will be handled appropriately by credit providers and credit reporting agencies.

The Government notes that, in line with the ALRC's views, the four data sets outlined in this recommendation will be made available without being subject to responsible lending obligations. The Government considers that the enhanced notification, data quality and dispute resolution requirements will provide sufficient protections to prevent the misuse of this information.

The Government notes that the binding industry code (outlined in recommendation 54-9) will also be an important mechanism to ensure consistency in how the four data sets are listed with credit reporting agencies. The Government will require the credit reporting industry to develop standards around how it lists the types of credit accounts as well as when a credit account is deemed to be closed. For example, in relation to account closure, confusion exists for individuals around whether some credit products are closed after final payment or whether these are ongoing lines of credit (such as interest free accounts). The Government encourages industry to provide clear information to customers about when a credit account will be deemed to be closed.

The Government proposes that the listing of the four data sets with credit reporting agencies will be permitted to occur in relation to existing accounts open at the time that amendments to the Privacy Act take effect. The Government does not consider there is justification for the argument that listing this type of information should only occur with respect to new accounts opened after the commencement of the amendments.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 55–2** Subject to Recommendation 55–3, the new *Privacy (Credit Reporting Information) Regulations* should also permit credit reporting information to include an individual's repayment performance history, comprised of information indicating:

- (a) whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not,
- (b) the number of repayment cycles the individual was in arrears.

**Response: Accept**

The Government notes there is significant debate over the possible effect that the inclusion of repayment history in credit reporting information could have on the provision of credit to consumers.

On balance, the ALRC found that the listing of repayment history would provide credit providers with an independent and easily obtainable source of information about an individual's willingness to repay and would also clearly demonstrate when individuals are under credit stress. The Government agrees with the ALRC's view that the predictive value of this extra data set will lead to more informed lending practices, which in turn will result in greater efficiency and effectiveness in consumer credit lending. The Government considers that the benefits this data set will provide to the Australian credit market, and in turn to individuals and credit providers, outweighs the possible adverse privacy effects.

The Government agrees to the introduction of the fifth data set of repayment history subject to the protections that the ALRC has outlined in recommendations 55-3 to 55-5. These protections will be supplemented by additional privacy protections, including in relation to data quality, which will be implemented across the credit reporting scheme.

The Government notes that, in line with recommendation 54-8, the effect of implementing recommendation 55-2 will be reviewed in due course. The review will determine whether further privacy protections are necessary to ensure that all the new comprehensive credit reporting data sets are being collected, used and disclosed appropriately.

Collection and use of repayment history information will be subject to the proposed commencement of the responsible lending obligations in the National Consumer Credit Protection Bill 2009 (see recommendation 55-3 below). However, the Government notes that some credit reporting stakeholders suggest that at the commencement of the repayment history amendments to the Privacy Act, credit reporting agencies should be able to list at least the previous 12 months' repayment history. Advocates have suggested that repayment history information should only be listed prospectively from the date these provisions commence.

The Government proposes that, in order to allow viable repayment history to be assessed from the commencement of the repayment history provisions, the period from when repayment history may be reported will commence six months after the release of this Government response. This will mean all credit consumers will be on notice that six months from the date of release of the Government's response, any repayment history on credit accounts may become available at a later date (ie when the repayment history provision commences) to a credit reporting agency and any other credit providers from which the

individual may seek credit.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 55–3** The Australian Government should implement Recommendation 55–2 only after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

**Response: Accept**

The Government acknowledges that the inclusion of repayment history in credit reporting information could assist in achieving more responsible lending of consumer credit. However, without a positive obligation to lend responsibly, the provision of repayment history data could mean that credit providers also take adverse credit risks based only on this information. It is therefore necessary that the inclusion of repayment history in credit reporting information should occur alongside appropriate responsible lending obligations.

In introducing the National Consumer Credit Protection Reform Package into Parliament, the Government has made a significant commitment to establishing enhanced protection for the provision of consumer credit. As part of these reforms, the Government is requiring all licensees under the reforms to comply with a set of responsible lending conduct requirements. These obligations will require licensees to ensure that they do not provide or suggest unsuitable credit to a consumer.

The Government is satisfied that the responsible lending conduct requirements in the Reform Package will provide a suitable framework to ensure that credit providers appropriately use information about an individual's repayment history (as outlined in recommendation 55-2).

As the responsible lending obligations will only be applicable to licensees subject to the National Consumer Credit Protection Bill 2009, the Government proposes that repayment history information should only be handled by credit providers subject to the obligations in that Bill.

The Government notes that the responsible lending obligations will not commence until January 2011 and therefore commencement of provisions about the use and disclosure of repayment history information will be subject to this same commencement date. The Government will consult with stakeholders on whether the 'plus four' data sets (ie the data sets outlined in recommendation 55-1) should be shared prior to the commencement of repayment history (noting that use and disclosure of these data sets will not be dependent on the commencement of the responsible lending obligations).

**Recommendation 55–4** The credit reporting code should set out procedures for reporting repayment performance history, within the parameters prescribed by the new *Privacy (Credit Reporting Information) Regulations*.

**Response: Accept in principle**

The Privacy Act will set out that only minimal information in relation to an individual's repayment history, in accordance with recommendation 55-2, should be collected by credit

reporting agencies and disclosed to credit providers. This information will not include information about account balances or specific repayment amounts.

The Government understands that the ALRC's intention in recommendation 55-2 was that a repayment would only be listed as 'missed' where the next repayment cycle had commenced and the previous payment had still not been made. The repayment cycle would be dependent on the timeframes set out in the credit contract. However, the Government notes that it may also be understood that a 'missed' payment would be deemed to occur prior to the next repayment cycle but within a defined period.

The Government notes that it should be clearly set out in the Privacy Act when a 'missed repayment' will be deemed to occur. The Government will seek further views from stakeholders about the preferred approach. If the latter approach is preferable, the Government proposes that the details of 'missed' payment timeframes should be set out in regulations.

The Government also considers that, given the significance that will be attributed to how repayment history is listed and the accompanying notices provided with this listing (see recommendation 56-11), these matters should be set out in regulations to the Privacy Act, rather than in the binding industry code. The Government proposes that the Privacy Act will set out the broad requirements applicable to listing repayment history in accordance with recommendation 55-2. Regulations would then outline issues about how and in what form the information will be listed, timing for missed payments and the notice requirements for repayment history. Regulations would also address other matters such as whether overdue payments which are re-negotiated for further scheduled payments should be listed and if so, how they should be listed.

The Government notes that the binding industry code will still play a part in determining other operational matters around repayment history that are not included in regulations, such as at what intervals a credit provider will list information with a credit reporting agency.

**Recommendation 55–5** The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of the information referred to in Recommendation 55–1 two years after the date on which a credit account is closed.

**Response: Accept**

In line with the overarching aim of credit reporting regulation to ensure that information is only maintained by credit reporting agencies and used by credit providers for as long as the information remains relevant to assessing an individual's credit worthiness, the Government considers that this retention period is appropriate.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

## 56. Collection and Permitted Content of Credit Reporting Information

**Recommendation 56–1** The new *Privacy (Credit Reporting Information) Regulations* should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information. This list should be based on the provisions of s 18E of the *Privacy Act*, subject to the changes set out in Recommendations 55–1, 55–2, 56–2 to 56–4, 56–6, 56–8 and 56–9.

### Response: Accept

The Government agrees that there continues to be a need to set out clearly what types of information may be collected by credit reporting agencies from credit providers and held as credit reporting information.

The categories of credit reporting information to be included in the exhaustive list will be restructured in line with the Government's response to the relevant ALRC recommendations. The list will be set out in amendments to the *Privacy Act* and will not be subject to change through regulations or determination by the Privacy Commissioner. The Government notes that the ALRC has undertaken a thorough review of what should be included as credit reporting information and that little justification has been provided to suggest that changes to the list should occur outside the *Privacy Act*.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the *Privacy Act*, not regulations.

**Recommendation 56–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies are not permitted to list overdue payments of less than a prescribed amount.

### Response: Accept

Regulations made under the *Privacy Act* will prescribe the minimum amount at which a credit reporting agency can list an overdue payment (ie a default). The amount should be based on balancing the need for credit providers to assess adequately the credit risk of an individual against the disproportionate consequences of listing less significant debts. It is necessary to prescribe this amount in regulations in order for it to be changed from time to time based on changing circumstances.

The Government proposes that, in line with current practices and in balancing the views of industry and advocate stakeholders, the prescribed amount should be \$100. Any defaults under this amount will not be able to be listed as credit reporting information.

The Government also proposes to consolidate the steps that must be taken to list a default (as outlined in the *Credit Reporting Code of Conduct* and the *Privacy Act*) and provide a simplified process in the *Privacy Act*.

**Recommendation 56–3** The new *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques.

**Response: Accept**

Information about presented and dishonoured cheques will not be included in the list of permitted contents allowed to be retained by credit reporting agencies as the information does not have a clear link to the assessment of credit and is increasingly irrelevant as a payment mechanism.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 56–4** The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index administered under the *Bankruptcy Regulations 1966* (Cth).

**Response: Accept in principle**

The Government acknowledges that it is important for credit providers to be able to identify whether an individual has entered bankruptcy administration so that the actual credit risk of the individual can be assessed more accurately. The Government notes that there is uncertainty about what can currently be listed as credit reporting information from the National Personal Insolvency Index (NPII) and strongly agrees that clarification is required.

The Government notes that, in accordance with its proposed reforms to ensure bankruptcy laws provide consumers with appropriate avenues for remedying indebtedness, credit reporting information should only include information that will provide an accurate picture of the individual's bankruptcy status.

The Government agrees that the following four categories of information about bankruptcy administration should be allowed to be included in credit reporting information:

- (i) a sequestration order by the Federal Court following the presentation of the debtor's petition;
- (ii) the acceptance of a debtor's petition by the Official Receiver, in lieu of a court order;
- (iii) a voluntary debt agreement; and
- (iv) a voluntary insolvency agreement.

These categories of information will provide clear advice to the credit provider as to whether the insolvent individual has entered a voluntary or mandatory bankruptcy administration, and the processes and procedures of that administration.

The Government also agrees that information about a proposal to make a debt agreement may be included in credit reporting information, as it would provide a credit provider with notice of the potential risks of lending to an individual. However, the Government considers that it would be appropriate to require information about the proposal to be removed from the individual's credit reporting information where the proposal was unsuccessful. Unlike finalised agreements or orders, information about proposed action on the NPII should only be retained for as long as that information remains valid (rather than the proposed retention

periods for finalised orders or agreements). This approach would be in line with recommendation 56-5.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 56–5** Credit reporting agencies should ensure that credit reports adequately differentiate the forms of administration identified on the National Personal Insolvency Index (NPII); and accurately reflect the relevant information recorded on the NPII, as updated from time to time.

**Response: Accept**

In order to assess appropriately the credit risk of an individual, it is important to clearly distinguish the type of bankruptcy administration to which the individual has been subject (ie whether it is mandatory or voluntary). The Government agrees it is important to ensure that this information is accurately reflected in credit reporting information.

The Government also agrees that as the National Personal Insolvency Index (NPII) is not a static document, credit reporting agencies should be under an obligation to ensure that information which is reported on from the NPII is up-to-date and accurately reflects the NPII's content. This would include ensuring that any information that is directly related to an order or agreement and which provides greater information about an individual's current credit risk is also included. For example, where a bankruptcy annulment occurs, it would be important that this is accurately reflected in the credit reporting information.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 56–6** The new *Privacy (Credit Reporting Information) Regulations* should allow for the listing of a 'serious credit infringement' based on the definition currently set out in s 18E(1)(b)(x) of the *Privacy Act*, amended so that the credit provider is required to have taken reasonable steps to contact the individual before reporting a serious credit infringement under s 18E(1)(b)(x)(c).

**Response: Accept**

The Government agrees that a credit provider should be required to demonstrate that it has taken reasonable steps to contact the individual where it intends to list a serious credit infringement based on a reasonable suspicion of non-compliance. This will ensure that a serious credit infringement can only be listed where there is a clear intent by the individual to avoid credit obligations, which would be demonstrated by the credit provider being unable to contact the individual after taking reasonable steps.

It is noted that this requirement would only apply to an activity defined under paragraph (c) of the definition of 'serious credit infringement' in subsection 6(1) of the Privacy Act. The Government considers that where a serious credit infringement is based on fraudulent activity, this activity alone is sufficient to justify listing a serious credit infringement.

Note: In line with the Government's response to recommendation 54-1, this recommendation

will be implemented in the Privacy Act, not regulations.

**Recommendation 56–7** The Office of the Privacy Commissioner should develop and publish guidance on the criteria that need to be satisfied before a serious credit infringement may be listed, including:

- (a) how to interpret ‘serious’ (for example, in terms of the individual’s conduct, and the period and amount of overdue payments);
- (b) how to establish whether reasonable steps to contact the individual have been taken;
- (c) whether a serious credit infringement should be listed where there is a dispute between the parties that is subject to dispute resolution; and
- (d) the obligations on credit providers and individuals in proving or disproving that a serious credit infringement has occurred.

**Response: Accept in principle**

The Government considers that it would be preferable given the level of concern over the application of a ‘serious credit infringement’ listing, that the elements outlined above be required by the Privacy Act to be addressed in the binding industry code. This will allow for the guidance to be binding on all those parties subject to the code and would provide a greater opportunity for industry, privacy and consumer advocates, and the Privacy Commissioner to work together to develop appropriate standards for the listing of serious credit infringements.

The Government notes that the Credit Reporting Code of Conduct as issued by the Privacy Commissioner provides guidance on the definition of ‘serious credit infringement’ and provides a useful model on how this could be addressed in the binding industry code.

**Recommendation 56–8** The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of ‘sensitive information’, as defined in the *Privacy Act*.

**Response: Accept**

The Government agrees that in order to create greater consistency in the Privacy Act, it would be sensible to place a prohibition on collecting sensitive information for credit reporting purposes in place of the current prohibition in section 18E(2).

Note: In line with the Government’s response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.



**Recommendation 56–9** The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals who the credit provider or credit reporting agency knows, or reasonably should know, to be under the age of 18.

**Response: Accept**

The Government acknowledges that there should be appropriate protections around the provision of credit to individuals under the age of 18 and that this protection should also be afforded in relation to credit reporting.

The Government is satisfied that on balance the enhanced protections that individuals under the age of 18 will receive in prohibiting the listing of their information with credit reporting agencies overrides the limited concerns raised that this may affect their ability to gain credit.

The Government would encourage guidance on when a credit provider or credit reporting agency would know or should reasonably know an individual's age as part of the binding industry code.

The effect of this prohibition will be that credit reporting information can only be recorded from the date when an individual turns 18. However where repayment history is recorded once the individual turns 18, information about when the account was opened (if it occurred before the individual turned 18) would be permitted to be recorded.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 56–10** The new *Privacy (Credit Reporting Information) Regulations* should provide, in addition to the other provisions of the 'Notification' principle, that at or before the time personal information to be disclosed to a credit reporting agency is collected about an individual, a credit provider must take such steps as are reasonable, if any, to ensure that the individual is aware of the:

- (a) identity and contact details of the credit reporting agency;
- (b) rights of access to, and correction of, credit reporting information provided by the regulations; and
- (c) actual or types of organisations, agencies, entities or persons to whom the credit reporting agency usually discloses credit reporting information.

**Response: Accept**

The Government agrees that more specific 'notification' requirements should be placed on credit providers to provide notice to individuals about not only the credit providers own information handling practices but also about specific practices of a credit reporting agency. The Government considers it is appropriate that this notification should occur at or before the time of the collection of the personal information to be disclosed to the credit reporting agency (ie at the time of applying for credit) rather than at any other time.

These 'notification' requirements will ensure that individuals are fully aware of how their information will be utilised in the credit reporting system. Notice of credit reporting agencies' practices is important given that individuals will most often not receive this information directly from credit reporting agencies.

The Government considers that these further notification requirements are reasonable and should not place an overly burdensome obligation on credit providers.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 56–11** The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit provider, before disclosing overdue payment information to a credit reporting agency, must have taken reasonable steps to ensure that the individual concerned is aware of the intention to report the information. Overdue payment information, for these purposes, means the information currently referred to in s 18E(b)(1)(vi) of the *Privacy Act*.

**Response: Accept with amendment**

The Government understands that there is confusion about when an individual should be notified that a default payment will be listed in their credit reporting information, and that often individuals are unaware that a default has been listed until they attempt to apply for new credit. Given the negative impacts that default listings have on an individual's credit worthiness, it is important that they be made aware that this information will be provided by a credit provider to a credit reporting agency.

The Government notes that the ALRC's proposed 'reasonable steps' test is intended to align with industry best practice that notification should occur just prior to a default being listed. This test does not attempt to dictate at what stage notice should be given as this would be dependent on the practices of each credit provider and any other notice obligations they are required to comply with in relation to consumer credit (for example, in relation to a default notice under the National Consumer Credit Protection Bill 2009). However, it is expected that any notice would be sufficiently connected in time to when the default is intended to be listed.

The Government also proposes, subject to further consultation with stakeholders, that this notification obligation would apply to credit providers who propose to list repayment history information which details 'missed' payments. The Government notes that the listing of 'missed' payments as part of repayment history will have a similar effect to default listings and so there should be appropriate notification to individuals that this information will be listed.

It is understood that generally credit providers will provide notification in overdue payment reminders that a default may be listed with a credit reporting agency where the payment remains overdue. In line with this approach, it is likely that any requirement to also notify about the potential listing of a 'missed' payment would not be overly burdensome for credit providers. It would be appropriate that procedural requirements around the notification of 'missed payments' would be outlined in greater detail in proposed regulations as set out in recommendation 55-4.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

## 57. Use and Disclosure of Credit Reporting Information

**Recommendation 57–1** The new *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information. This list should be based on the provisions of Part IIIA of the *Privacy Act*, which currently authorise the use and disclosure by credit reporting agencies and credit providers of personal information contained in credit information files, credit reports and reports relating to credit worthiness (ss 18L, 18K and 18N).

### Response: Accept

The Government agrees that the current drafting in Part IIIA of the *Privacy Act* in relation to the way that credit providers and credit reporting agencies can use and disclose credit reporting information is overly complicated and confusing. The Government is committed to redrafting the use and disclosure provisions to continue to allow the current practices of credit reporting agencies, credit providers, mortgage and trade insurers and debt collectors. These permitted uses and disclosures will be outlined in a clearer and more consistent way.

However, the Government considers that it is still necessary to have clearly defined uses and disclosures in relation to credit reporting information which would be narrower than those allowed under the ‘use and disclosure’ principle. This is important to ensure that credit reporting information does not become increasingly used for purposes unrelated to assessing credit applications or managing a credit account as currently outlined in Part IIIA. It is intended that any revised provisions will provide sufficient detail to ensure that information handling practices in relation to credit reporting information do not extend beyond uses and disclosures as currently defined in the *Privacy Act*.

Note: In line with the Government’s response to recommendation 54-1, this recommendation will be implemented in the *Privacy Act*, not regulations.

**Recommendation 57–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit reporting agency or credit provider may use or disclose credit reporting information for a secondary purpose related to the assessment of an application for credit or the management of an existing credit account, where the individual concerned would reasonably expect such use or disclosure.

### Response: Not accept

The Government does not support the ALRC’s recommendation as it would allow credit reporting information to be used and disclosed for a number of unknown purposes. This in turn would significantly reduce the value of the credit reporting provisions to promote transparency and consistency for individuals concerning appropriate uses and disclosures of credit reporting information. In effect, the ALRC’s recommendation would be contrary to the requirement to have defined uses and disclosures as outlined in recommendation 57-1 and would undermine the purpose of having specific provisions which operate in addition to the general ‘use and disclosure’ principle. While the ALRC proposed to limit the discretion in relation to secondary uses and disclosures by specifically defining the primary purpose, the Government is not convinced that greater use or disclosure of credit reporting information should be subject to a broad discretion exercised by credit providers or credit reporting agencies.

However, the Government accepts that there may be circumstances where the use or disclosure of credit reporting information goes beyond the purposes agreed to in recommendation 57-1 and notes that amendments to the Privacy Act would not necessarily allow efficient recognition of those uses or disclosures. In order to permit additional uses and disclosures in a timely yet transparent way, the Government will provide that regulations can prescribe additional uses and disclosures to those in recommendation 57-1.

Additional uses and disclosures of credit reporting information will be permitted where the use or disclosure can be shown to be in the public interest as well as being for the benefit of the individuals whose credit reporting information will be used and disclosed. The Government's consideration of these issues would be subject to appropriate public consultation with the credit reporting industry, consumer and privacy advocates and the Privacy Commissioner. Where the Government considers that the use or disclosure is justified in these circumstances, it could prescribe that credit reporting information may be used and/or disclosed for a prescribed purpose by either specified credit providers or credit reporting agencies or any credit provider or credit reporting agency.

The Government understands that a key concern for both credit reporting agencies and credit providers in supporting recommendation 57-2 was that it would provide an ability to conduct research (including statistical modelling and data analysis) in relation to credit reporting information where it related to the assessment or management of credit and was for the benefit of the public.

In addition to the permitted uses and disclosures under recommendation 57-1, the Government will also allow for credit providers or credit reporting agencies to use and disclose de-identified credit reporting information for research purposes that are deemed to be in the public interest and have a sufficient connection to the credit reporting system. Research would also be required to be conducted in accordance with rules developed by the Privacy Commissioner.

Such rules would detail requirements on notifying affected individuals and the public about the research, steps to ensure that the research does not unjustifiably impact on an individual's privacy (including where consent should be obtained) and how the research can be used and disclosed.

**Recommendation 57–3** The new *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing, including the pre-screening of direct marketing lists.

**Response: Accept in part**

The Government agrees that, even in light of its response to recommendation 57-2, it is important to make clear that credit reporting information should not be used or disclosed in any circumstances for the purposes of direct marketing. This will ensure that the permitted uses and disclosures of credit reporting information are interpreted in line with this prohibition.

The Government acknowledges the ALRC's views on the use or disclosure of credit reporting information for the purpose of pre-screening direct marketing lists. However, the Government considers that, on balance, the use or disclosure of credit reporting information for the purposes of pre-screening should be expressly permitted, but only for the purpose of excluding adverse credit risks from marketing lists. Pre-screening would be subject to specific requirements including the following:

- (i) only negative credit reporting information can be used or disclosed for the purpose of pre-screening direct marketing lists;
- (ii) individuals must be given specific notice at the time of collection of their personal information that it may be used for pre-screening;
- (iii) individuals must be given the opportunity to opt-out of having their credit reporting information used for pre-screening;
- (iv) individuals removed from direct marketing lists by pre-screening cannot be specifically identified for other direct marketing;
- (v) credit providers, credit reporting agencies, mailing houses, or any other organisation involved in pre-screening must maintain auditable evidence to verify compliance with the pre-screening restrictions;
- (vi) credit reporting agencies must maintain evidence that is available to individuals which records the actual use, if any, of their credit reporting information for the purposes of pre-screening;
- (vii) pre-screening must only be available to credit providers as defined under Part IIIA of the Act and who are subject to the National Consumer Credit Protection Bill 2009; and
- (viii) any organisations involved in pre-screening must be subject to the general requirements of the Privacy Act, if they are not already so covered.

The Government recognises the importance of any organisation involved in pre-screening (including mailing houses) maintaining adequate evidence to demonstrate compliance with the pre-screening requirements. The Government considers that this evidence must be made available for auditing by the Office of the Privacy Commissioner as required. The Government encourages the Office to provide guidance to organisations involved in pre-screening on compliance with this requirement.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 57–4** The use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) should be authorised expressly under the AML/CTF Act.

**Response: Accept in principle**

The Government agrees that, subject to adequate privacy protections being put in place, credit reporting agencies should be allowed to use and disclose credit reporting information for the purposes of identity verification under the AML/CTF Act. The Attorney-General's Department has undertaken consultations to determine how this recommendation can be implemented in the most privacy enhancing way.

**Recommendation 57–5** The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to prohibit for a specified period the disclosure by a credit reporting agency of credit reporting information about them without their express authorisation.

**Response: Accept**

The Government strongly agrees that there should be measures in place to allow individuals to highlight to potential credit providers in their credit reporting information that they are a victim of fraud, including identity theft. These measures could assist in preventing credit reporting information from being used to perpetuate fraud.

The Government agrees that the Privacy Act should allow individuals, who have a reasonable belief that they are or are about to be victims of fraud, to request that a credit reporting agency restrict access to their credit reporting information. Where credit providers seek access to credit reporting information that has been restricted, credit reporting agencies would be required to advise the credit provider that they are unable to release information due to the individual's concerns about fraud. An individual would be able to consent to their credit reporting information being released where it is for legitimate purposes.

The Government agrees with the ALRC's proposal that, where a credit provider provides credit during the period that access is restricted and it is shown that the credit was provided for illegitimate purposes, the credit provider would be prohibited from listing a default or serious credit infringement that occurs as a result of that provision of credit.

The onset of fraud, particularly identity theft, often requires immediate action and the Government notes that it may be difficult for individuals to demonstrate to credit reporting agencies their reasonable belief that fraud has or is likely to occur. The Government therefore proposes that the credit reporting agency should restrict access to the individual's credit reporting information immediately at the individual's request and that the access restriction should remain in place for a period of 14 days. In order to extend the restriction beyond this initial period, an individual would be required to demonstrate to the credit reporting agency that they have a reasonable belief that fraud has or is likely to occur. This would not necessarily require court-based evidence, but could include a statutory declaration by the individual or advice from the individual's financial institution.

The extension of the access restriction beyond this initial period would be subject to reasonable periods as determined within the binding industry code. The code should also set out other procedural requirements about notifying the individual of the effect of restricting access, the initial period in which access will be restricted, subsequent notifications that an access restriction period is ending, and how a credit provider should be informed of why the access restriction is in place.

**Recommendation 57–6** There should be no equivalent in the new *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information in ‘reports’ related to credit worthiness. The use and disclosure limitations should apply only to ‘credit reporting information’ as defined for the purposes of the new regulations.

**Response: Not accept**

Credit providers should continue to be restricted from disclosing ‘credit worthiness’ information in accordance with the protections in section 18N of the *Privacy Act*. This is particularly important in relation to information which is similar to that maintained by credit reporting agencies or which directly relates to an individual’s existing credit account. The Government considers that there should be consistency around how this information is disclosed and assurances for individuals that it will not be disclosed in an inappropriate way. For example, the Government considers that information that relates to an individual’s repayment history or credit account limit or balance should only be disclosed by a credit provider to another credit provider where an individual specifically consents to this disclosure.

The Government acknowledges that the current definition of a report about an individual’s ‘credit worthiness’ is too broad and covers information that would be adequately protected by the general ‘use and disclosure’ privacy principle. The definition will therefore be revised to only apply to information that is similar to information maintained by a credit reporting agency (in accordance with recommendation 56-1) or information that is about an individual’s credit accounts. It is not intended to cover information about an individual’s income or employment details.

## 58. Data Quality and Security

**Recommendation 58–1** The new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a state or a territory from bringing proceedings against the individual to recover the amount of the overdue payment; or where any relevant statutory limitation period has expired.

### Response: Accept

Allowing the listing in credit reporting information of a default payment that is otherwise unrecoverable would be inconsistent with the public policy of providing legal protection against the recovery of debt in certain circumstances. It should be made clear that statute-barred debts should not be allowed to be listed in credit reporting information.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 58–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt—such as by entering into a scheme of arrangement with the credit provider—an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information for the full five-year period permissible under the regulations.

### Response: Accept

The Government considers it is appropriate that, where a default or serious credit infringement has been listed in an individual's credit reporting information and the individual enters a new scheme of arrangement relating to that listing, any future default under that arrangement may be listed separately. This will provide evidence that an individual continues to be under credit stress and put credit providers on notice.

This will apply to schemes of arrangement as currently defined in the Office of the Privacy Commissioner's guidance to the Credit Reporting Code of Conduct and will only apply to schemes that are as a result of a previous default or serious credit infringement listing.

The Government notes that the listing of a default that occurs under a new scheme of arrangement will be subject to the same requirements that apply to the listing of defaults more generally. For example, the same notification requirements would apply as outlined in recommendation 56-11.

It is also intended to make clear in the Privacy Act that notes about schemes of arrangements can be included in credit reporting information (in line with the provisions in the Credit Reporting Code of Conduct).

The Government has indicated that it will also be considering the application of schemes of arrangement in relation to the listing of repayment history when making regulations to clarify the application of that data set (see recommendation 55-4).

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.



**Recommendation 58–3** The credit reporting code should promote data quality by setting out procedures to ensure consistency and accuracy of credit reporting information. These procedures should deal with matters including:

- (a) the timeliness of the reporting of credit reporting information;
- (b) the calculation of overdue payments for credit reporting purposes;
- (c) obligations to prevent the multiple listing of the same debt;
- (d) the updating of credit reporting information; and
- (e) the linking of credit reporting information relating to individuals who may or may not be the same individual.

**Response: Accept**

The Government understands that there are concerns about the differing approaches that members of the credit reporting industry are taking to ensure data quality of credit reporting information. In particular, the ALRC expressed strong concerns about inconsistency in the practices relating to the listing of default payments.

The Government agrees that operational issues in relation to ensuring data quality should be addressed by industry, in consultation with consumer and privacy groups and the Privacy Commissioner, in the binding industry code.

**Recommendation 58–4** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

- (a) enter into agreements with credit providers that contain obligations to ensure the quality and security of credit reporting information;
- (b) establish and maintain controls to ensure that only credit reporting information that is accurate, complete and up-to-date is used or disclosed;
- (c) monitor data quality and audit compliance with the agreements and controls; and
- (d) identify and investigate possible breaches of the agreements and controls.

**Response: Accept**

It is important for both credit reporting agencies and credit providers to take proactive steps to establish practices which maintain the data quality and security of credit reporting information. Given that credit reporting agencies play a key role in managing credit reporting information it is appropriate that they be charged with the responsibility to develop appropriate agreements.

The Government expects that the agreements established by credit reporting agencies and credit providers will expand upon the procedures which are outlined in relation to 'accuracy of information' in the current Credit Reporting Code of Conduct. The Government notes that these aspects of the Code of Conduct should be included in the binding industry code, where necessary.

The Government notes that this recommendation will supplement credit providers' and credit reporting agencies' compliance with the general Privacy Principles in relation to 'data quality' and 'data security'. These principles overlap with paragraphs 18G(a) and (b) of the Privacy Act and these paragraphs will not need to be repeated in the revised credit reporting

provisions. However, the Privacy Act will continue to require separately that credit providers and credit reporting agencies take reasonable steps in accordance with paragraph 18G(c) to prevent unauthorised use or disclosure of credit reporting information where provided to a third party.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 58–5** The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.

**Response: Accept**

The Government agrees that the current retention periods for retaining and disclosing certain credit reporting information remain valid. The Government's response to recommendation 58-6 should also be noted.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 58–6** The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of information about voluntary arrangements with creditors under Parts IX and X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.

**Response: Accept with amendment**

The Government agrees that, in line with its reforms to modernise the *Bankruptcy Act 1966* to ensure that individuals can effectively access a fresh start to their financial affairs, the five-year retention period for information about voluntary arrangements is sufficient. This adequately balances the need to ensure that individuals who have faced financial difficulty are able to re-engage in the economy with the need for industry to assess credit risk.

However, the Government is not convinced that there is sufficient justification to warrant a difference in reporting periods between voluntary arrangements or bankruptcy by creditor's petition (ie a bankruptcy 'order'). Insolvent individuals should not be discriminated against on the basis that they have elected for the most appropriate method to remedy their financial circumstances. These individuals should be afforded an opportunity to rectify their financial circumstances equal to that enjoyed by those that entered voluntary arrangements.

The Government therefore proposes that all bankruptcy information should be listed for the same period of five years. This period would be capable of being extended in line with the period of an individual's bankruptcy administration. For example, where bankruptcy is extended for up to eight years it could be listed in an individual's credit reporting information for that period. A bankruptcy 'order' would therefore be able to be listed for five years or the ordered period of bankruptcy, whichever is greater.

The Government also considers that where an individual successfully completes a voluntary

arrangement early, they should have the ability to request that a credit reporting agency attach a note to the listing of the arrangement to reflect this fact.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

## 59. Access and Correction, Complaint Handling and Penalties

**Recommendation 59–1** The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to obtain access to credit reporting information based on the provisions currently set out in s 18H of the *Privacy Act*.

### Response: Accept

This is in line with the approach that the credit reporting provisions in the Privacy Act should only set out those requirements that are different or more specific to the general Privacy Principles. The access rights set out in section 18H should be replicated in amendments to the Act, as it is not appropriate for the exceptions in the general ‘access and correction’ principle to apply to credit reporting information.

The correction rights in the general ‘access and correction’ principle closely align with the current requirements in section 18J. Therefore it will be appropriate that credit reporting agencies and credit providers are only subject to the general correction requirements in the ‘access and correction’ principle.

The Government notes that currently the Credit Reporting Code of Conduct sets out more detailed requirements in terms of when credit reporting agencies and credit providers should provide access to, and correct, credit reporting information. These matters should continue to be outlined as necessary in the binding industry code. The Privacy Act will require that the code set out matters in relation to when and how access and correction should be provided for and the timeliness of the transactions.

Note: In line with the Government’s response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must provide individuals, on request, with one free copy of their credit reporting information annually.

### Response: Accept in principle

It is important to ensure that individuals have a statutory right to receive, on request and within a reasonable timeframe, a free copy of their credit reporting information from a credit reporting agency. The Government understands that currently individuals have the ability to gain a free copy of their credit reporting information and that this practice should be mandated.

The Government considers that the binding industry code should set out the appropriate timeframes in which free copies should be provided to individuals. This will allow industry to determine in consultation with privacy and consumer advocates what is deemed a reasonable timeframe based on factors such as the urgency of a request (for example, where a dispute arises) along with the costs associated in providing a free copy. The Government notes that it may be appropriate to set out different timeframes for accessing a free copy based on the reason for the access request and whether it is reasonable that individuals will always receive a free copy in certain circumstances. These are all matters which it would be appropriate for the credit reporting industry to determine.

The binding industry code should also set out the form in which access should be given. The Government strongly encourages credit reporting agencies to take reasonable steps to

provide access to credit reporting information, including free copies, electronically.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–3** The new *Privacy (Credit Reporting Information) Regulations* should provide an equivalent of s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised for a credit-related purpose by a person authorised in writing.

**Response: Accept**

The Government agrees that it is necessary to continue to adopt this stringent approach to restricting third party access to credit reporting information. This will assist in ensuring that credit reporting information does not become accessed for non-credit related purposes which would in turn undermine the role of credit reporting regulation.

The Government notes that this recommendation is not intended to place onerous restriction on those third parties who are assisting individuals to communicate with a credit reporting agency or a credit provider (such as through a translator or the National Relay Service). The Government would encourage the Office of the Privacy Commissioner to provide guidance on appropriate third party access to credit reporting information.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–4** The new *Privacy (Credit Reporting Information) Regulations* should provide that, where a credit provider refuses an application for credit based wholly or partly on credit reporting information, it must notify an individual of that fact. These notification requirements should be based on the provisions currently set out in s 18M of the *Privacy Act*.

**Response: Accept**

The notification requirement in section 18M of the Privacy Act plays an important role in developing transparency around the operation of the credit reporting system. Its continued application will ensure that individuals are aware of all the relevant issues to assist them in understanding how they can access their credit reporting information and which elements of the information may have led to the refusal of credit.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–5** The new *Privacy (Credit Reporting Information) Regulations* should provide that:

- (a) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint in a fair, efficient and timely manner;
- (b) a credit reporting agency should refer to a credit provider for resolution complaints about the content of credit reporting information provided to the agency by that credit provider; and
- (c) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint, it must inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

**Response: Accept in part**

Given that an individual is likely to deal with a number of organisations when trying to resolve a dispute about credit reporting information, the Government strongly agrees there should be clear requirements about who should take responsibility to attempt to resolve the dispute.

In this recommendation the ALRC has reversed the obligation for resolving disputes and placed the onus on the relevant credit provider who is likely to have sufficient access to information in order to deal with the dispute. However, the Government is concerned that this approach could still result in an individual having to take several steps before ownership of the dispute settles with the credit provider. This would occur particularly where the individual relies on details from a notice provided under recommendation 59-4 to contact the credit reporting agency at first instance.

The Government considers that a more balanced approach is that the obligation for attempting to resolve the dispute should lie with whichever party the individual first makes a complaint (whether it be the credit provider to which the listing relates or the credit reporting agency). This will place a clear onus on the first contacted party to take measures to resolve the dispute and will ensure that the individual themselves is not required to go back and forth between the parties.

Either party would then be required to take the necessary steps to attempt to resolve the complaint, including liaising with and obtaining information from the other relevant body (ie the credit reporting agency would be required to consult with the credit provider and would need to take reasonable steps to obtain information to resolve the dispute). Either party could act as the intermediary for the individual to assist them, to the extent possible, to resolve the dispute. The party would then need to advise all other relevant parties, including the individual, of the outcome of the investigation and the further steps the individual could take through either external dispute resolution (see recommendation 59-7) or by making a complaint to the Privacy Commissioner if they are not satisfied with the outcome.

The Government notes that where a credit reporting agency or credit provider determines that corrections need to be made to the individual's credit reporting information, they should take steps to advise the other party, along with other relevant credit reporting agencies who may have listed the information, of the corrections. This will be in accordance with the general 'access and correction' principle.

The Privacy Act will outline these overarching requirements. However, this approach to dispute resolution will only work effectively where there are robust procedures established between credit providers and credit reporting agencies to deal with initial complaints they

receive. The Government considers that the binding industry code should play an important part in formalising these procedures across the industry. The code would set out matters such as when a 'dispute' has been raised by an individual, the timeliness in responding to the individual, providing information about the party responsible for considering the dispute, procedures for establishing appropriate contact officers in credit reporting agencies and credit providers, and information sharing procedures.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–6** The new *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given, if an individual's application for credit is refused based wholly or partly on credit reporting information, should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.

**Response: Accept**

The Government agrees that in addition to the requirements in recommendation 59-4, the individual should also be provided with short form advice on the mechanisms available if they have a complaint about their credit reporting information. This would include noting that either the relevant credit provider or credit reporting agency should be contacted at first instance prior to making a complaint to the Privacy Commissioner.

The Government notes that it would be appropriate for the binding industry code to outline what type of information should be provided to the individual.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–7** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit providers only may list overdue payment or repayment performance history where the credit provider is a member of an external dispute resolution scheme recognised by the Privacy Commissioner.

**Response: Accept with amendment**

The Government considers that there is significant justification to extend the requirement to be a member of a recognised external dispute resolution (EDR) scheme to all credit reporting agencies and credit providers that list any information about an individual in credit reporting information.

With the introduction of comprehensive credit reporting and the possible adverse impacts that other information such as the listing of serious credit infringements can have on an individual, the Government considers it would be more consistent to apply this requirement to all those credit providers that actively list information. This will ensure that individuals who have concerns that information is incorrectly listed will have access to efficient external dispute resolution.

The Government notes that credit providers and credit reporting agencies will be able to be members of any EDR scheme that is recognised by the Privacy Commissioner. In line with

recommendation 49-2, the Privacy Commissioner will have a broad discretion to recognise a number of EDR schemes that are officially established under legislation, approval by the Australian Securities and Investments Commission or through other independent and accountable processes. It is expected that many credit providers and credit reporting agencies will already be members of an applicable EDR scheme and that this should not result in an overly onerous burden for the industry.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–8** The new *Privacy (Credit Reporting Information) Regulations* should provide that, within 30 days, evidence to substantiate disputed credit reporting information must be provided to the individual, or the matter referred to an external dispute resolution scheme recognised by the Privacy Commissioner. If these requirements are not met, the credit reporting agency must delete or correct the information on the request of the individual concerned.

**Response: Accept**

This recommendation will ensure that the onus of proving the accuracy or appropriateness of a listing in an individual's credit reporting information lies with credit providers and credit reporting agencies. It is also likely to assist in encouraging the credit reporting industry to resolve disputes as quickly and efficiently as possible.

The Government understands that mechanisms will need to be put in place to determine at what point in time a complaint will be deemed to have been made and the appropriate notice that should be provided to the individual about the dispute process. In line with recommendation 59-5, these matters should be addressed as part of the binding industry code. The Government will consider other matters, such as the interaction of this recommendation with frivolous or vexatious complaints, as part of making this amendment to the Privacy Act.

The Government notes the concern that even where subject to an external dispute resolution (EDR) process, the disputed listing could continue to remain in the individual's credit reporting information. To ensure there is sufficient transparency around the fact that the listing is in dispute, it will be a requirement that where a dispute is referred to an EDR scheme, a note to this effect is associated with the disputed listing.

Note: In line with the Government's response to recommendation 54-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 59–9** The *Privacy Act* should be amended to remove the credit reporting offences and allow a civil penalty to be imposed as provided for by Recommendation 50–2.

**Response: Accept**

The Government agrees that civil offences are more appropriate for the breach of any provisions in relation to credit reporting.



## PART H – HEALTH SERVICES AND RESEARCH

### 60. Regulatory Framework for Health Information

**Recommendation 60–1** Health information should be regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles (UPPs), and regulations under the *Privacy Act*—the new *Privacy (Health Information) Regulations*. The new *Privacy (Health Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model UPPs.

**Response: Not accept**

In line with the Government's response to recommendation 5-1, the Government believes that the substantive rights and obligations in relation to the handling of health information, and other personal information, should be set out in the primary legislation.

Where an ALRC recommendation refers to the *Privacy (Health Information) Regulations* and the Government accepts the recommendation's intent, the Government will implement that recommendation in the primary legislation (the *Privacy Act*) unless otherwise stated.

There should also be provision for specific regulations to be made where necessary. For example, in recommendation 62-2 the Government proposes including a power to exclude certain entities from the definition of 'health service' in regulation.

The ALRC has made several other recommendations in relation to the content of the suggested *Privacy (Health Information) Regulations*. The Government response to those recommendations should be read subject to its response not to accept this recommendation (60-1).

**Recommendation 60–2** The Office of the Privacy Commissioner should publish a document bringing together the model Unified Privacy Principles (UPPs) and the additions set out in the new *Privacy (Health Information) Regulations*. This document should contain a complete set of the model UPPs as they relate to health information.

**Response: Not accept**

This recommendation is not accepted as the Government does not accept recommendation 60-1.

**Recommendation 60–3** The Office of the Privacy Commissioner—in consultation with the Department of Health and Ageing and other relevant stakeholders—should develop and publish guidelines on the handling of health information under the *Privacy Act* and the new *Privacy (Health Information) Regulations*.

**Response: Accept in principle**

The Government encourages the development and publication of appropriate guidance by the Office of the Privacy Commissioner, noting that the decision to provide guidance is a

matter for the Privacy Commissioner.

As the Government does not accept recommendation 60-1, such guidance would be on the application of the Privacy Act and the Privacy Principles to health information, rather than on health privacy regulations (as proposed by the ALRC).

## 61. Electronic Health Information Systems

**Recommendation 61–1** If a national Unique Healthcare Identifiers (UHIs) or a national Shared Electronic Health Records (SEHR) scheme goes forward, it should be established under specific enabling legislation. This legislation should address information privacy issues, such as:

- (a) the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;
- (b) the eligibility criteria, rights and requirements for participation in the UHI and SEHR schemes by health consumers and health service providers, including consent requirements;
- (c) permitted and prohibited uses and linkages of the personal information held in the systems;
- (d) permitted and prohibited uses of UHIs and sanctions in relation to misuse; and
- (e) safeguards in relation to the use of UHIs, including providing that it is not necessary to use a UHI in order to access health services.

### **Response: Accept in principle**

The Australian Health Ministers' Conference (AHMC) announced in its 5 March 2009 communiqué that, consistent with the Council of Australian Governments (COAG) agreement that all Australian residents will be allocated an Individual Healthcare Identifier (IHI), Health Ministers have agreed to continuing consultations on privacy protections that will be necessary to underpin this important health initiative.

The AHMC announced the start of public consultations on the IHI and health privacy protections in its 13 July 2009 communiqué. A report on the outcomes will be provided to COAG later in 2009.

The Government agrees with the necessity of privacy protections for any national Unique Healthcare Identifiers (UHIs) or national Shared Electronic Health Records (SEHR) scheme. The substance of these protections and details of matters to be addressed in legislation, such as those matters outlined by the ALRC in paragraphs (a) to (e) of its recommendation, should be subject to specific future consultation as any UHI or SEHR scheme goes forward.

## 62. The Privacy Act and Health Information

**Recommendation 62–1** The definition of ‘health information’ in the *Privacy Act* should be amended to make express reference to the *physical, mental or psychological* health or disability of an individual.

### **Response: Accept**

The Government agrees that the definition of ‘health information’ should be amended to make clear that it includes information in relation to physical, mental and psychological health.

**Recommendation 62–2** The Privacy Act should be amended to define a ‘health service’ as:

- (a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:
  - (i) assess, predict, maintain or improve the individual’s physical, mental or psychological health or status;
  - (ii) diagnose the individual’s illness, injury or disability; or
  - (iii) prevent or treat the individual’s illness, injury or disability or suspected illness, injury or disability;
- (b) a health-related disability, palliative care or aged care service;
- (c) a surgical or related service; or
- (d) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

### **Response: Accept with amendment**

The definition of ‘health service’ should also expressly exclude activities performed for reasons other than care or treatment, such as life, health or other forms of insurance.

The Privacy Act should also be amended to provide that the Governor-General may make regulations, consistent with the Act, to exclude, whether specifically or by class, organisations or agencies from the definition of providing a ‘health service’, where it is not appropriate for those entities to be included in the definition.

These amendments will give further effect to the policy intent of the ‘health service’ definition proposed by the ALRC.

### 63. Privacy (Health Information) Regulations (Health-specific reforms to the Privacy Principles)

**Recommendation 63–1** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the ‘Collection’ principle, an agency or organisation that provides a health service may collect health information from an individual, or a person responsible for the individual, about third parties when:

- (a) the collection of the third party’s information is necessary to enable the health service provider to provide a health service directly to the individual; and
- (b) the third party’s information is relevant to the family, social or medical history of that individual.

#### **Response: Accept**

This amendment would overcome the need for the Privacy Commissioner to make further Public Interest Determinations (PIDs) on this matter (currently PIDs 10 and 10A). Given the likelihood that there will remain a strong public interest in such collections being permitted, it is appropriate that a permanent authority be established for this practice.

Note: In line with the Government’s response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–2** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the ‘Collection’ principle, an agency or organisation that is a health service provider may collect health information about an individual if the information is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose.

#### **Response: Accept**

This amendment would provide an authority for collection that effectively mirrors the existing authority to disclose health information for directly related purposes that are within individuals’ reasonable expectations (currently National Privacy Principle 2.1(a), proposed Unified Privacy Principle 5.1(a)).

Note: In line with the Government’s response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–3** National Privacy Principles (NPPs) 2.4 to 2.6—dealing with the disclosure of health information by a health service provider to a person who is responsible for an individual—should be moved to the new *Privacy (Health Information) Regulations*. The new regulations should provide that, in addition to the other provisions of the ‘Use and Disclosure’ principle, an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual, if the individual is incapable of giving consent to the disclosure and all the other circumstances currently set out in NPP 2.4 are met. In addition, the new regulations should:

- (a) be expressed to apply to both agencies and organisations;
- (b) not refer to a health service provider who may make a disclosure under these provisions as a 'carer'; and
- (c) define 'a person who is responsible for an individual' as:
  - (i) a parent, child or sibling of the individual;
  - (ii) a spouse or de facto partner of the individual;
  - (iii) a relative of the individual who is a member of the individual's household;
  - (iv) a substitute decision maker authorised by a federal, state or territory law to make decisions about the individual's health;
  - (v) a person who has an intimate personal relationship with the individual;
  - (vi) a person nominated by the individual to be contacted in case of emergency; or
  - (vii) a person who is primarily responsible for providing support or care to the individual.

In considering whether to disclose an individual's health information to a person who is responsible for an individual and who is under the age of 18, a health service provider should consider, on a case-by-case basis, that person's maturity and capacity to understand the information.

**Response: Accept with amendment**

To address potential confusion around the meaning of 'incapable of giving consent', the Government proposes that this should be clarified to cover circumstances where an individual is incapable of:

- (i) understanding the general nature and effect of disclosing the information; or
- (ii) indicating whether he or she agrees to the disclosure.

To reflect the diversity of individuals' carer arrangements, the Government considers that paragraph (c)(vii) should not be limited to the person 'primarily' responsible for support or care only. Guidance will be important to assist in the application in practice of the definition of 'a person who is responsible for an individual'.

Note: In line with the Government's response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–4** The *Privacy Act* should be amended to provide a definition of 'de facto partner' in the following terms: 'de facto partner' means a person in a relationship as a couple with another person to whom he or she is not married.

**Response: Not accept**

Following amendments to both Acts in 2008, the Privacy Act imports the definition of 'de facto partner' as provided in the *Acts Interpretation Act 1901*. To maintain consistency across legislation, the Government does not propose to change the existing definition.

**Recommendation 63–5** The new *Privacy (Health Information) Regulations* should include provisions similar to those set out in National Privacy Principle 2.1(ea) on the use and disclosure of genetic information where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. These regulations should apply to both agencies and organisations. Any use or disclosure under the new regulations should be in accordance with rules issued by the Privacy Commissioner.

**Response: Accept with amendment**

The Government agrees that the Privacy Act should continue to include an equivalent exception to National Privacy Principle (NPP) 2.1(ea) on genetic disclosures, which would apply to agencies and organisations that provide a health service.

Given the specialist clinical and privacy expertise likely to be required in developing rules on genetic disclosures, the Government believes that the current framework should be retained, whereby the National Health and Medical Research Council (NHMRC) issues the rules, to be approved by the Privacy Commissioner before becoming operational.

To facilitate such disclosures, the Privacy Act should be amended (such as by way of specific exceptions) to permit a 'health service' provider to:

- collect the contact details of a patient's genetic relatives (which may constitute 'health information'); or
- use those contact details when that information is already in the health practitioner's possession

where that information is necessary in order to disclose genetic information about the patient to the relatives in accordance with the NPP 2.1(ea) equivalent provision (or where the patient has consented to the disclosure).

As noted in the response to recommendation 25-3, the Government considers that, for consistency, a 'serious threat' should refer to 'life, health or safety'.

Note: In line with the Government's response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–6** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, if an individual is denied access to his or her own health information by an agency on the basis that providing access would, or could reasonably be expected to, endanger the life or physical safety of any person, or by an organisation on the basis that providing access would be reasonably likely to pose a serious threat to the life or health of any individual:

- (a) the agency or organisation must advise the individual that he or she may nominate a suitably qualified health service provider ('nominated health service provider') to be given access to the health information;
- (b) the individual may nominate a health service provider and request that the agency or organisation provide the nominated health service provider with access to the information;
- (c) if the agency or organisation does not object to the nominated health service provider, it must provide the nominated health service provider with access to the health information within a reasonable period of time; and

- (d) the nominated health service provider may assess the grounds for denying access to the health information and may provide the individual with access to the information to the extent that the nominated health service provider is satisfied that to do so, in the case of an agency, would not, or could not be reasonably expected to, endanger the life or physical safety of any person and, in the case of an organisation, would not be reasonably likely to pose a serious threat to the life or health of any individual.

If the agency or organisation objects to the nominated health service provider and refuses to provide the nominated health service provider with access to the information, the individual may nominate another suitably qualified health service provider, or may lodge a complaint with the Privacy Commissioner alleging an interference with privacy.

**Response: Accept with amendment**

Under paragraph (a) above, the nominated health service provider should be 'suitably qualified and appropriate' for the purposes of being an intermediary in the given instance. This is intended to avoid conflicts of interest and other circumstances where an intermediary is qualified, but not appropriate.

As noted in the response to recommendation 25-3, the Government considers that, for consistency, a 'serious threat' should refer to 'life, health or safety'.

The ALRC's recommendations use different terminology for agencies and organisations, due to existing exceptions to deny access under the *Freedom of Information Act 1982* (FOI Act). Where practicable and appropriate the Government will emphasise ongoing consistency of phrasing in the Privacy Act and FOI Act.

Note: In line with the Government's response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–7** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Data Security' principle, where an agency or organisation that provides a health service is sold, amalgamated or closed down, and an individual health service provider will not be providing health services in the new agency or organisation, or an individual health service provider dies, the provider, or the legal representative of the provider, must take reasonable steps to:

- (a) make individual users of the health service aware of the sale, amalgamation or closure of the health service, or the death of the health service provider; and
- (b) inform individual users of the health service about proposed arrangements for the transfer or storage of individuals' health information.

**Response: Accept with amendment**

These obligations should also apply to health services where a partnership dissolves, or a practice otherwise de-merges or disaggregates.

Note: In line with the Government's response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.



**Recommendation 63–8** (a) The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the ‘Access and Correction’ principle, where an individual requests that an agency or organisation that is a health service provider transfers the individual’s health information to another health service provider, the agency or organisation must respond within a reasonable time and transfer the information.

(b) Other elements of the ‘Access and Correction’ principle relating to access should apply to a request for transfer from one health service provider to another, amended as necessary.

**Response: Accept**

The ‘other elements’ referred to in paragraph (b) of the recommendation include:

- exceptions permitting the denial of access (modified as necessary to refer to denial of information transfer);
- permitting charges for transfer, provided they are not excessive (and do not merely relate to the act of making the request to transfer); and
- transferring health information in the manner requested by the individual (including summary form).

Note: In line with the Government’s response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–9** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the ‘Collection’ principle and the ‘Use and Disclosure’ principle, an agency or organisation may collect, use or disclose health information where necessary for the funding, management, planning, monitoring, or evaluation of a health service where:

- (a) the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual or from which the individual would not be reasonably identifiable;
- (b) it is unreasonable or impracticable for the agency or organisation to seek the individual’s consent before the collection, use or disclosure; and
- (c) the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.

**Response: Accept with amendment**

The term ‘planning’ (of a health service) should be omitted.

Paragraph (a) should be accepted.

In paragraph (b), the word ‘unreasonable’ should be omitted, as it may unnecessarily and unintentionally broaden the effect of the exception. If the impact of seeking consent to the collection, use or disclosure would unduly prejudice the objective of an appropriate management activity, then seeking consent could be considered ‘impracticable’. (This is consistent with the requirements for research under recommendation 65-5.)

In relation to paragraph (c), the relevant rules should be made by the National Health and Medical Research Council (NHMRC) and subject to the Privacy Commissioner’s approval by legislative instrument. The NHMRC has relevant clinical expertise and is well placed to

develop such rules. The role of the Privacy Commissioner ensures an appropriate balance between clinical matters and privacy.

Note: In line with the Government's response to recommendation 60-1, this recommendation will be implemented in the Privacy Act, not regulations.

**Recommendation 63–10** The *Privacy Act* should be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, or evaluation of a health service.

**Response: Not accept**

As in recommendation 63-9, these rules should be made by the National Health and Medical Research Council (in consultation with relevant stakeholders) and approved by the Privacy Commissioner. The approval should be in the form of a legislative instrument.

## 65. Research: Recommendations for Reform

**Recommendation 65–1** (a) The Privacy Commissioner should issue one set of rules under the research exceptions to the ‘Collection’ principle and the ‘Use and Disclosure’ principle to replace the *Guidelines under Section 95 of the Privacy Act 1988* and the *Guidelines Approved under Section 95A of the Privacy Act 1988*.

(b) The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the ‘Collection’ and ‘Use and Disclosure’ principles—that is, the ‘Research Rules’.

(c) Those elements of the *National Statement on Ethical Conduct in Human Research* dealing with privacy should be aligned with the Privacy Act and the Research Rules to minimise confusion for institutions, researchers and Human Research Ethics Committees.

### **Response: Accept with amendment**

One set of research rules should be issued, though these should be made by the National Health and Medical Research Council in conjunction with other appropriate bodies such as the Australian Research Council and Universities Australia, rather than by the Privacy Commissioner.

The Privacy Commissioner should have an approval function for the research rules. That approval should be in the form of a legislative instrument.

Paragraph (c) of this recommendation should be accepted.

**Recommendation 65–2** The *Privacy Act* should be amended to extend the arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

### **Response: Accept**

Forms of human research beyond those relating to health and medical research can serve important public interests. Provided that appropriate protections are adopted, the Privacy Act should permit the collection, use and disclosure of personal information without consent for the purpose of important human research in certain circumstances.

Appropriate protections should include:

- that the exception may only be relied upon where consent is impracticable;
- the activity is subject to institutional ethical oversight of research proposals; and
- the public interest in a research proposal substantially outweighs the public interest in protecting privacy.

**Recommendation 65–3** The *Privacy Act* should be amended to provide that ‘research’ includes the compilation or analysis of statistics.

**Response: Accept**

This provides a simplified form of the wording which is more appropriate for use in the Privacy Principles.

**Recommendation 65–4** The research exceptions to the ‘Collection’ principle and the ‘Use and Disclosure’ principle should provide that, before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*.

**Response: Accept with amendment**

The test should be that the Human Research Ethics Committee is satisfied that the public interest in the research activity *substantially* outweighs the public interest in maintaining the level of privacy. The requirement of substantiality ensures that there is a clear balance in favour of the research activity progressing. Such clarity is appropriate in circumstances where individuals’ personal information will be handled without their consent.

**Recommendation 65–5** The research exceptions to the ‘Collection’ principle and the ‘Use and Disclosure’ principle should include a provision stating that it must be ‘unreasonable or impracticable’ to seek consent from individuals to the collection, use or disclosure of their personal information before that information may be used without consent for the purposes of research.

**Response: Accept in part**

The term ‘unreasonable’ should be omitted, as it may unnecessarily and unintentionally broaden the effect of the exception. If seeking consent to the collection, use or disclosure would unavoidably and substantially prejudice the research objective, to the extent of rendering the research invalid, then seeking consent could be considered ‘impracticable’.

**Recommendation 65–6** The National Health and Medical Research Council, the Australian Research Council and Universities Australia should amend the *National Statement on Ethical Conduct in Human Research* to state that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by a Human Research Ethics Committee.

**Response: Accept**

A research activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, should be assessed by a Human Research Ethics Committee, properly constituted in accordance with the *National Statement on Ethical Conduct in Human Research*.

This would provide important assurance that the proposed research mechanism is not being used for unintended purposes.

**Recommendation 65–7** The Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements imposed under the *Privacy Act* on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.

**Response: Accept**

The reporting obligations contained in the research rules should serve a clear purpose.

The Government has agreed that the relevant research rules should be made by the National Health and Medical Research Council and other appropriate expert bodies and approved by the Privacy Commissioner (see the Government's response to recommendation 65-1).

Accordingly, consultation is encouraged between those entities in order to review the reporting requirements for research activities under the *Privacy Act*. The form of this consultation and review is a matter for those entities.

**Recommendation 65–8** The research exception to the ‘Collection’ principle should provide that an agency or organisation may collect personal information, including sensitive information, about an individual where all of the following conditions are met:

- (a) the collection is necessary for research;
- (b) the purpose cannot be served by the collection of information that does not identify the individual;
- (c) it is unreasonable or impracticable for the agency or organisation to seek the individual’s consent to the collection;
- (d) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the National Statement on Ethical Conduct in Human Research as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act; and
- (e) the information is collected in accordance with the Research Rules, to be issued by the Privacy Commissioner.

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

**Response: Accept with amendment**

In regard to paragraph (c), ‘unreasonable’ should be omitted (see the response to recommendation 65-5).

In regard to paragraph (d), the public interest in the proposed activity should be required to ‘substantially outweigh’ the public interest in maintaining privacy protections (see the response to recommendation 65-4).

The research rules referred to in paragraph (e) should be made by the National Health and Medical Research Council and other relevant bodies, and approved by the Privacy Commissioner (see the response to recommendation 65-1).

**Recommendation 65–9** The research exception to the ‘Use and Disclosure’ principle should provide that an agency or organisation may use or disclose personal information where all of the following conditions are met:

- (a) the use or disclosure is necessary for research;
- (b) it is unreasonable or impracticable for the agency or organisation to seek the individual’s consent to the use or disclosure;
- (c) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the National Statement on Ethical Conduct in Human Research as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act;
- (d) the information is used or disclosed in accordance with the Research Rules, to be issued by the Privacy Commissioner; and
- (e) in the case of disclosure—the agency or organisation reasonably believes that the

recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable.

**Response: Accept with amendment**

In regard to paragraph (b), 'unreasonable' should be omitted (see the response to recommendation 65-5).

In regard to paragraph (c), the public interest in the proposed activity should be required to 'substantially outweigh' the public interest in maintaining privacy protections (see the response to recommendation 65-4).

The research rules referred to in paragraph (d) should be made by the National Health and Medical Research Council and other relevant bodies, and approved by the Privacy Commissioner (see the response to recommendation 65-1).

## 66. Research: Databases and Data Linkage

**Recommendation 66–1** The Privacy Commissioner should address the following matters in the Research Rules:

- (a) in what circumstances and under what conditions it is appropriate to collect, use or disclose personal information without consent for inclusion in a database or register for research purposes; and
- (b) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

### **Response: Accept in principle**

The research rules should be made by the National Health and Medical Research Council (NHMRC) and other appropriate bodies, and approved by the Privacy Commissioner (see the response to recommendation 65-1). The Government accepts that the research rules should address the issues proposed in relation to databases and registers. This is a matter for the NHMRC and other entities responsible for the rules.

**Recommendation 66–2** Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should conduct a Privacy Impact Assessment to ensure that the privacy risks involved are assessed and adequately managed in the design and implementation of the project.

### **Response: Accept in principle**

While conducting privacy impact assessments should be encouraged as good practice, it is not proposed to be obligatory. The Office of the Privacy Commissioner could assist in promoting this practice by producing targeted guidance to assist agencies and organisations in these circumstances. The decision to provide guidance is a matter for the Privacy Commissioner.

**Recommendation 66–3** The Research Rules, to be issued by the Privacy Commissioner, should address the circumstances in which, and the conditions under which, it is appropriate to collect, use or disclose personal information without consent in order to identify potential participants in research.

### **Response: Accept in principle**

The research rules should be made by the National Health and Medical Research Council (NHMRC) and other appropriate bodies, and approved by the Privacy Commissioner (see the response to recommendation 65-1). The Government accepts that the research rules should address the issues proposed in relation to 'sample acquisition' for research purposes. This is a matter for the NHMRC and other entities responsible for the rules.