The Senate

Legal and Constitutional Affairs Legislation Committee

Privacy Amendment (Enhancing Privacy Protection) Bill 2012 [Provisions]

September 2012

ISBN: 978-1-74229-691-3

This document was printed by the Senate Printing Unit, Department of the Senate, Parliament House, Canberra.

MEMBERS OF THE COMMITTEE

Members

Senator Patricia Crossin, **Chair**, ALP, NT

Senator Gary Humphries, **Deputy Chair**, LP, ACT

Senator Sue Boyce, LP, QLD

Senator Mark Furner, ALP, QLD

Senator Louise Pratt, ALP, WA

Senator Penny Wright, AG, SA

Secretariat

Ms Julie Dennett	Committee Secretary
Ms Monika Sheppard	Inquiry Secretary
Mr CJ Sautelle	Senior Research Officer
Ms Ann Palmer	Principal Research Officer
Ms Elise Williamson	Administrative Officer

With assistance from:

Ms Toni Matulick	Inquiry Secretary, Environment and Communications Committee secretariat

Suite S1.61	Telephone:	(02) 6277 3560
Parliament House	Fax:	(02) 6277 5794
CANBERRA ACT 2600	Email:	legcon.sen@aph.gov.au

TABLE OF CONTENTS

ABBREVIATIONS

AAM	Abacus-Australian Mutuals
ABA	Australian Bankers' Association
ACCAN	Australian Communications Consumer Action Network
ADMA	Australian Direct Marketing Association
AFC	Australian Finance Conference
AIC	Australian Insurance Council
AIC Act	*Australian Information Commissioner Act 2010* (Cth)
ALRC	Australian Law Reform Commission
ANZ	ANZ Banking Group Limited
APEC	Asia-Pacific Economic Cooperation
APPs	Australian Privacy Principles
APP entities	Commonwealth agencies and certain private sector organisations
ARCA	Australasian Retail Credit Association
Bill	Privacy Amendment (Enhancing Privacy Protection) Bill 2012
CALC	Consumer Action Law Centre
CCLCNSW	Consumer Credit Legal Centre (NSW)
CCLSWA	Consumer Credit Legal Service (WA)
Commissioner	Australian Information Commissioner
committee	Senate Legal and Constitutional Affairs Legislation Committee
credit reporting provisions	proposed new Part IIIA of the *Privacy Act 1988* (Cth)
Department	Attorney-General's Department

DIAC	Department of Immigration and Citizenship
EDR	external dispute resolution
EM	Explanatory Memorandum
EWON	Energy & Water Ombudsman NSW
FIA	Fundraising Institute of Australia
FOS	Financial Ombudsman Service
F&PA committee	Senate Finance and Public Administration Legislation Committee
F&PA inquiry	Senate Finance and Public Administration Legislation Committee's Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation
IPPs	Information Privacy Principles
Law Council	Law Council of Australia
National Consumer Credit Protection Act	*National Consumer Credit Protection Act 2009* (Cth)
NPPs	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
OPC	Office of the Privacy Commissioner
PID	Public Interest Determination
Privacy Act	*Privacy Act 1988* (Cth)
Privacy Foundation	Australian Privacy Foundation
RIS	Regulation Impact Statement

RECOMMENDATIONS

Recommendation 1

6.13 The committee recommends that the application of the exception in proposed APP 2.2(b) be clarified to make it clear that APP 2.1 does not apply where it is impracticable for the APP entity to deal with 'individuals who have not identified themselves or who have used a pseudonym'.

Recommendation 2

6.27 The committee recommends that, to avoid confusion, the subheading to proposed APP 7.1 in item 104 of Schedule 1 of the Bill be amended to read 'Use or disclosure' or 'Direct marketing', rather than 'Prohibition on direct marketing'.

Recommendation 3

6.31 The committee recommends that proposed APP 7.2 and APP 7.6 in item 104 of Schedule 1 of the Bill be amended to ensure consistency with the notification requirement in APP 7.3, and enable individuals the opportunity to opt-out of direct marketing communications at any time.

Recommendation 4

6.37 The committee recommends that proposed APP 8.2(b) in item 104 of Schedule 1 of the Bill be amended to require an entity to inform an individual of the practical effect and potential consequences of any informed consent by the individual to APP 8.1 not applying to the disclosure of the individual's personal information to an 'overseas recipient'.

Recommendation 5

6.38 The committee recommends that the Explanatory Memorandum to the Bill be revised to clearly explain that an entity will be required to inform an individual of the practical effect and potential consequences of any informed consent by the individual to APP 8.1 not applying to the disclosure of the individual's personal information to an 'overseas recipient'.

Recommendation 6

6.42 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill to clearly explain the enforcement-related functions and activities of the Department of Immigration and Citizenship, as justification for the classification of the 'Immigration Department' as an 'enforcement body' in item 17 of Schedule 1 of the Bill.

Recommendation 7

6.43 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill to clearly explain the scope and intended application of the terms 'surveillance activities', 'intelligence gathering activities', and 'monitoring activities' in item 20 of Schedule 1 of the Bill.

Recommendation 8

6.47 The committee recommends that the provisions contained in item 82 of Schedule 1 of the Bill and for each Australian Privacy Principle which contains a 'permitted general situation' or 'permitted health situation' exception, a note should be added at the end of the relevant principle to cross-reference proposed new section 16A of the *Privacy Act 1988* and/or proposed new section 16B of the *Privacy Act 1988*, as appropriate.

Recommendation 9

6.48 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill to explain the intended scope and application of the 'diplomatic or consular functions or activities' exception set out in item 6 in the table to proposed new subsection 16A(1) of the Privacy Act in item 82 of Schedule 1 of the Bill.

Recommendation 10

6.59 The committee recommends that proposed new subsection 6Q(1) in item 69 of Schedule 2 of the Bill be amended to require an appropriate amount of time, such as 14 days, to have elapsed from the date of a written notice before a default listing can occur.

Recommendation 11

6.60 The committee recommends that the written notification in proposed new subsection 6Q(1) in item 69 of Schedule 2 of the Bill be amended to include a warning about the potential for a default listing by a 'credit provider' in the event that an overdue amount is not paid within a set period of time.

Recommendation 12

6.61 The committee recommends that proposed new subparagraph 6Q(1)(d)(i) in item 69 of Schedule 2 of the Bill be amended to reflect $300, or such higher amount as the Australian Government considers appropriate, as the minimum amount for which a consumer credit default listing can be made.

Recommendation 13

6.62 The committee recommends that the Office of the Australian Information Commissioner, in formulating guidelines under proposed new section 26V in item 72 of Schedule 2 of the Bill, include as a criterion the timeframe within which an individual's 'default information' can be listed by a 'credit provider'.

Recommendation 14

6.63 The committee recommends that the Office of the Australian Information Commissioner, in formulating guidelines under proposed new section 26V in item 72 of Schedule 2 of the Bill, include a requirement for credit providers to fully consider an application for financial difficulty assistance under the *National Consumer Credit Protection Act 2009* before an individual's 'default information' can be listed.

Recommendation 15

6.78 The committee recommends that the Australian Government consider prohibiting the re-identification of 'credit reporting information' which has been de-identified for research purposes in accordance with proposed new subsection 20M(2) in item 72 of Schedule 2 of the Bill, and whether a proportionate civil penalty should apply to any breach of that prohibition.

Recommendation 16

6.81 The committee recommends that proposed new sections 20T and 21V in item 72 of Schedule 2 of the Bill be amended to:

- **create an obligation for the recipient of a request to take reasonable steps to have the information corrected by the entity which holds the disputed information;**
- **create an obligation for the entity which holds the disputed information to correct the information within 30 days, if satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; and**
- **create an obligation for the recipient of a request to notify the individual about the outcome of their request if that request has been determined by another entity which holds the disputed information.**

Recommendation 17

6.84 The committee recommends that the regulations made pursuant to section 100 of the *Privacy Act 1988* provide a mechanism for 'credit reporting bodies' and 'credit providers' who have received a request for the correction of an individual's personal information to note on the individual's credit file that a correction is under investigation, with the notation to be removed upon completion of that investigation.

Recommendation 18

6.86 The committee recommends that the Bill be amended to enable a 'credit reporting body' or 'credit provider' to correct an individual's personal information in exceptional circumstances, such as in the case of natural disasters, bank error, fraud, medical incapacity, and mail theft.

Recommendation 19

6.93 The committee recommends that the commencement date for the Bill remain at nine months after the Bill receives Royal Assent in order to provide certainty for all relevant stakeholders.

Recommendation 20

6.96 The committee recommends that, before the Bill's commencement date, the Office of the Australian Information Commissioner – in consultation with the Attorney-General's Department, as appropriate – develop and publish material informing consumers of the key changes to privacy legislation as proposed by the Bill, and providing guidance to Commonwealth agencies and private sector organisations to ensure compliance with the new legislative requirements.

Recommendation 21

6.98 Subject to the preceding recommendations, the committee recommends that the Senate pass the Bill.

CHAPTER 1

Introduction

Background and purpose of the Bill

1.1 On 23 May 2012, the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Bill) was introduced into the House of Representatives by the Attorney-General, the Hon. Nicola Roxon MP.[1] On 19 June 2012, the Senate referred the Bill to the Legal and Constitutional Affairs Legislation Committee (committee) for inquiry and report by 14 August 2012.[2] The reporting date was subsequently extended to 25 September 2012.[3] The House of Representatives passed the Bill on 17 September 2012,[4] and the Bill was introduced into the Senate on 18 September 2012.[5]

1.2 The Bill amends the *Privacy Act 1988* (Privacy Act) to implement the Australian Government's first stage response to the 2008 Australian Law Reform Commission's (ALRC) report, *For Your Information: Australian Privacy Law and Practice*.[6] According to the Explanatory Memorandum (EM), the Bill:

- creates the Australian Privacy Principles, a single set of privacy principles applying to both Commonwealth agencies and private sector organisations;
- introduces more comprehensive credit reporting with improved privacy protections, and revises provisions relating to credit reporting;
- introduces new provisions on privacy codes and the credit reporting code; and
- clarifies and improves the functions and powers of the Australian Information Commissioner.[7]

---

1 House of Representatives, *Votes and Proceedings*, No. 107-23 May 2012, p. 1471.

2 *Journals of the Senate*, No. 92-19 June 2012, p. 2528.

3 *Journals of the Senate*, No. 100-14 August 2012, p. 2719; *Journals of the Senate*, No. 108-11 September 2012, p. 2932; *Journals of the Senate*, No. 114-20 September 2012, p. 3044.

4 House of Representatives, *Votes and Proceedings*, No. 132-17 September 2012, p. 1794.

5 *Journals of the Senate*, No. 112-18 September 2012, p. 3014.

6 Explanatory Memorandum (EM), p. 1. Also see 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, p. 9, available at: http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf (accessed 7 September 2012). A summary table of the Australian Government's response to each of the 197 recommendations being addressed as part of the first stage response is provided at pp 15-19 of the response.

7 EM, p. 1.

1.3 The introduction of the Bill follows a number of reviews into Australia's privacy legislation. In addition to the ALRC, reviews have, for example, been conducted by the Office of the Privacy Commissioner (now the Office of the Australian Information Commissioner)[8] and the Senate Legal and Constitutional Affairs References Committee.[9] In 2010-2011, the Senate Finance and Public Administration Legislation Committee examined Exposure Drafts of the current Bill.[10]

1.4 In her second reading speech, the Attorney-General stated that the Bill is one of the most significant developments in privacy law reform and will bring Australia's privacy protection framework into the modern era.[11]

Overview of the Bill

1.5 The Bill contains six schedules, each of which proposes amendments relating to a particular subject and associated matters (such as definitions):

- Schedule 1 – Australian Privacy Principles;
- Schedule 2 – Credit reporting;
- Schedule 3 – Privacy codes;
- Schedule 4 – Other amendments to the Privacy Act, including the functions and powers of the Australian Information Commissioner;
- Schedule 5 – Consequential amendments to other Commonwealth Acts; and
- Schedule 6 – Application, transitional and savings provisions.

---

8 Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005, available at: http://www.privacy.gov.au/materials/types/reports/view/6049 (accessed 7 September 2012).

9 Senate Legal and Constitutional Affairs References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/completed_inquiries/2004-07/privacy/report/index.htm (accessed 7 September 2012).

10 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/report_part1/index.htm (accessed 7 September 2012);

Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/report_part2/index.htm (accessed 7 September 2012).

11 *House of Representatives Hansard*, 23 May 2012, p. 5210.

1.6 Schedules 1 to 4 of the Bill amend the Privacy Act; Schedule 5 of the Bill amends 55 other Commonwealth Acts; and Schedule 6 of the Bill sets out provisions relating to both the Privacy Act and the 55 other Commonwealth Acts.

Australian Privacy Principles

1.7 Schedule 1 of the Bill abolishes the Information Privacy Principles, which apply to the public sector, and the National Privacy Principles, which apply to the private sector.[12] It replaces them with the Australian Privacy Principles (APPs), which are reproduced in Appendix 1 to this report.[13] The APPs will be a single set of thirteen privacy principles in relation to which Commonwealth agencies and certain private sector organisations (APP entities) must comply as relevant.[14]

1.8 The APPs will be inserted into the Privacy Act in a new Schedule 1[15] and will be grouped in five Parts. Each part deals with a particular set of principles:

- Part 1 – principles that require APP entities to consider the privacy of personal information, including ensuring that personal information is managed in an open and transparent way (APP 1, APP 2);
- Part 2 – principles that deal with the collection of personal information, including dealing with unsolicited personal information (APP 3, APP 4, APP 5);
- Part 3 – principles about how APP entities deal with personal information and government-related identifiers, including the use and disclosure of personal information and identifiers, and direct marketing (APP 6, APP 7, APP 8, APP 9);
- Part 4 – principles about the integrity of personal information (quality and security) (APP 10, APP 11); and
- Part 5 – principles that deal with access to, and the correction of, personal information (APP 12, APP 13).[16]

12 Item 82 of Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Bill).

13 Proposed new section 14 of the *Privacy Act 1988* (Privacy Act); item 82 of Schedule 1 of the Bill.

14 Proposed new section 15 of the Privacy Act; item 82 of Schedule 1 of the Bill; proposed new Schedule 1 of the Privacy Act; item 104 of Schedule 1 of the Bill.

15 Item 104 of Schedule 1 of the Bill.

16 EM, pp 2 and 72-73.

1.9 The EM contains a detailed explanation of each APP;[17] however, individual APPs will be described and discussed in later chapters of the committee's report only where relevant to the examination of particular issues and concerns raised in the inquiry.

1.10 Schedule 1 of the Bill also sets out a range of provisions relating to the APPs (such as new definitions). Several key terms or concepts will be amended, including: the term 'personal information'; the meaning of 'reasonably necessary'; the term 'sensitive information'; the issue of consent; and the requirement to 'take reasonable steps'.[18]

Credit reporting

1.11 Schedule 2 of the Bill amends provisions throughout the Privacy Act which deal with credit reporting.[19] The credit reporting provisions (currently set out in Part IIIA of the Privacy Act) regulate the handling and maintenance of certain kinds of personal information regarding consumer credit that is intended to be used wholly or primarily for domestic, family or household purposes.[20]

1.12 Item 72 of Schedule 2 of the Bill completely revises the credit reporting provisions, with the repeal of current Part IIIA of the Privacy Act and the creation of new Part IIIA of the Privacy Act. Proposed new Part IIIA will deal with the privacy of credit reporting related information in six substantive Divisions:

- Divisions 2 and 3 contain rules that apply to 'credit reporting bodies' and 'credit providers' pertinent to their handling of information related to credit reporting;
- Division 4 contains rules that apply to 'affected information recipients' in relation to their handling of 'regulated information';
- Division 5 deals with complaints to 'credit reporting bodies' and 'credit providers' about acts or practices that might breach certain provisions of new Part IIIA of the Privacy Act or the registered credit reporting code;
- Division 6 deals with entities that obtain 'credit reporting information' or 'credit eligibility information' by false pretence, or when they are not authorised to do so under new Part IIIA of the Privacy Act; and

17 EM, pp 73-89.

18 EM, pp 53-54. Also see item 36 of Schedule 1 of the Bill and items 41-42 of Schedule 1 of the Bill, which define, respectively, the key terms 'personal information' and 'sensitive information'.

19 EM, p. 90.

20 EM, p. 2.

- Division 7 provides for compensation orders and other orders to be made by the Federal Court of Australia or the Federal Magistrates Court.[21]

1.13 By way of summary, the EM states that the main credit reporting reforms are:

- introduction of more comprehensive credit reporting to provide additional information about an individual's ongoing credit arrangements;
- changes to the obligations relating to the retention of different categories of personal information;
- introduction of specific rules to deal with pre-screening of credit offers and the freezing of access to an individual's personal information in cases of suspected identity theft or fraud;
- provision of additional consumer protections by enhancing obligations and processes dealing with notification, data quality, access and correction, and complaints; and
- changes to the regulation of credit reporting to more accurately reflect the information flows within the system and the general obligations set out in the APPs.[22]

1.14 Other amendments in Schedule 2 relate to matters of interpretation, including general definitions in subsection 6(1) of the Privacy Act[23] and key definitions relating to credit reporting.[24]

1.15 In her second reading speech, the Attorney-General stated that the Bill is the first major reform to credit reporting since its introduction in 1990 and identified the ways in which banks, financial institutions, the finance and credit industry, businesses and individuals will benefit from the reforms:

> Banks and financial institutions will be able to see more accurate and positive information…[meaning] more families can access credit. And it will mean the banks can assess credit risks more accurately…
>
> These reforms will give the Australian finance and credit industry more information—with the appropriate privacy protections—so that they can make more accurate risk assessments. More information—which will need to be more up to date and accurate under this bill—will assist both consumers and the credit reporting industry. It is expected that these reforms will lead to decreased levels of over-indebtedness and then lower credit default rates.

---

21 Proposed new section 19 of the Privacy Act; item 72 of Schedule 2 of the Bill. Division 1 sets out an introduction to Part IIIA.

22 EM, p. 92.

23 Items 2-65 of Schedule 2 of the Bill.

24 Proposed new Division 2 of Part II of the Privacy Act; item 69 of Schedule 2 of the Bill.

> For Australian businesses and the credit industry more comprehensive credit reporting will enable better management of capital and growth targets, improve credit decisions and enhance the effectiveness of how credit reporting agencies collect data.
>
> It is also expected to lead to more competition and efficiency in the credit market, which may in turn lead to more affordable credit and mortgage insurance for families and first home buyers.[25]

Privacy codes

1.16 Schedule 3 of the Bill repeals current Part IIIAA of the Privacy Act,[26] which sets out provisions relating to privacy codes, and inserts a new Part IIIB.[27] Proposed new Part IIIB of the Privacy Act will provide for information privacy codes of practice (APP code)[28] and credit reporting codes of practice (CR code).[29]

1.17 An APP code may be developed by an 'APP code developer' or, in certain circumstances, by the Australian Information Commissioner (Commissioner).[30] An APP code: must set out how one or more of the APPs are to be applied or complied with; may impose requirements in addition to those imposed by the APPs; and may deal with other specified matters.[31] Once an APP code has been developed, an 'APP code developer' may apply to the Commissioner for registration of the code.[32] The Commissioner may register an APP code developed by an 'APP code developer' or by the Commissioner.[33]

1.18 The process for the development of a CR code is similar to the development of an APP code. A CR code may be developed by a 'CR code developer' on request from the Commissioner or, in certain circumstances, by the Commissioner.[34] A CR code:

- must set out how one or more of the credit reporting provisions are to be applied or complied with;
- must deal with matters required or permitted by the credit reporting provisions to be provided for by the 'registered CR code';

---

25 *House of Representatives Hansard*, 23 May 2012, pp 5210-5211.

26 Item 28 of Schedule 3 of the Bill.

27 Item 29 of Schedule 3 of the Bill.

28 Proposed new Division 2 of new Part IIIB of the Privacy Act; item 29 of Schedule 3 of the Bill.

29 Proposed new Division 3 of new Part IIIB of the Privacy Act; item 29 of Schedule 3 of the Bill.

30 Proposed new sections 26E and 26G of the Privacy Act; item 29 of Schedule 3 of the Bill.

31 Proposed new section 26C of the Privacy Act; item 29 of Schedule 3 of the Bill.

32 Proposed new section 26F of the Privacy Act; item 29 of Schedule 3 of the Bill.

33 Proposed new section 26H of the Privacy Act; item 29 of Schedule 3 of the Bill.

34 Proposed new sections 26P and 26R of the Privacy Act; item 29 of Schedule 3 of the Bill.

- must bind all 'credit reporting bodies'; and
- may deal with other specified matters.[35]

1.19 Once a CR code has been developed, the 'CR code developer' may apply to the Commissioner for registration of the code.[36] The Commissioner may register a CR code developed by a 'CR code developer' or by the Commissioner.[37]

1.20 Registered APP codes and registered CR codes will be disallowable legislative instruments[38] and, if bound by one of these codes, APP entities and credit reporting entities will be prohibited from doing an act, or engaging in a practice, which breaches that code.[39] A breach of a registered code will constitute an interference with the privacy of an individual,[40] which will be subject to investigation by the Commissioner under Part 5 of the Privacy Act (Investigations).

1.21 Schedule 3 of the Bill also amends provisions relating to interpretation (including the insertion of new definitions);[41] and sets out provisions relating to a register of codes which have been registered by the Commissioner in accordance with new Part IIIB of the Privacy Act, guidelines relating to codes and the review of the operation of registered codes.[42]

Other amendments to the Privacy Act

1.22 Schedule 4 of the Bill makes several amendments to the Privacy Act, including: insertion of an objects clause;[43] reform of the functions and powers of the Commissioner; and related matters (for example, provisions about interferences with privacy).[44]

---

35 Proposed new section 26N of the Privacy Act; item 29 of Schedule 3 of the Bill.

36 Proposed new section 26Q of the Privacy Act; item 29 of Schedule 3 of the Bill.

37 Proposed new section 26S of the Privacy Act; item 29 of Schedule 3 of the Bill.

38 Proposed new subsections 26B(2) and 26M(2) of the Privacy Act; item 29 of Schedule 3 of the Bill.

39 Proposed new sections 26A and 26L of the Privacy Act; item 29 of Schedule 3 of the Bill.

40 Proposed new paragraphs 13(1)(b) and 13(2)(b) of the Privacy Act; item 42 of Schedule 4 of the Bill.

41 Items 1 to 26 of Schedule 3 of the Bill.

42 Proposed new Division 4 of new Part IIIB of the Privacy Act; item 29 of Schedule 3 of the Bill.

43 Proposed new section 2A of the Privacy Act; item 1 of Schedule 4 of the Bill. For example, two of the eight objects are (a) to promote the protection of the privacy of individuals; and (b) to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities.

44 EM, p. 4.

1.23 In particular, current Division 2 of Part IV of the Privacy Act – which sets out the functions of the Commissioner – will be repealed[45] and will be replaced by new provisions relating to general, guidance-related, monitoring-related and advice-related functions of the Commissioner.[46]

1.24 According to the Attorney-General, the Commissioner's powers have been substantially amended to provide individuals with enforceable remedies for breaches of privacy.[47]

1.25 Schedule 4 of the Bill will insert several new provisions into the Privacy Act, allowing the Commissioner to:

- conduct an assessment relating to an APP entity or credit reporting entity's maintenance and handling of personal information, and direct an agency to provide a 'privacy impact assessment' about a proposed activity or function involving the handling of personal information;[48]
- accept a written undertaking given by an entity to take, or refrain from taking, specified actions to ensure compliance with the Privacy Act, and apply to the Federal Court of Australia or the Federal Magistrates Court for enforcement of the undertaking (including orders for compensation);[49]
- recognise an external dispute resolution scheme;[50]
- investigate, on the Commissioner's own initiative, acts or practices which might be an interference with the privacy of an individual or which might breach an APP;[51]
- conciliate complaints;[52]
- make inquiries of persons other than the respondent to a complaint;[53] and
- include in a determination any order that is considered necessary or appropriate.[54]

---

45 Item 54 of Schedule 4 of the Bill.

46 Proposed new sections 27-28B of the Privacy Act; item 54 of Schedule 4 of the Bill. Associated definitions are also amended in Schedule 4 of the Bill.

47 *House of Representatives Hansard*, 23 May 2012, p. 5211. Also see EM, pp 4-5.

48 Proposed new sections 33C and 33D of the Privacy Act; item 64 of Schedule 4 of the Bill.

49 Proposed new sections 33E and 33F of the Privacy Act; item 64 of Schedule 4 of the Bill.

50 Proposed new section 35A of the Privacy Act; item 66 of Schedule 4 of the Bill.

51 Items 78 and 79 of Schedule 4 of the Bill.

52 Proposed new section 40A of the Privacy Act; item 80 of Schedule 4 of the Bill.

53 Item 90 of Schedule 4 of the Bill.

54 Proposed new subsection 52(3A) of the Privacy Act; item 111 of Schedule 4 of the Bill.

1.26 Schedule 4 of the Bill also extends the extra-territorial operation of the Privacy Act, together with registered APP codes and registered CR codes, to organisations and small business operators with an 'Australian link'.[55]

1.27 Schedule 4 of the Bill inserts a new Part VIB into the Privacy Act.[56] The new Part VIB, which deals with civil penalty orders, will prohibit entities from contravening a 'civil penalty provision'.[57] The Commissioner may apply to the Federal Court of Australia or the Federal Magistrates Court for an order that an entity, which is alleged to have contravened a 'civil penalty provision', pay the Commonwealth a pecuniary penalty.[58] Proposed new section 13G of the Privacy Act makes special provision for serious and repeated interferences with the privacy of an individual.[59]

1.28 The Attorney-General noted:

> Penalties range from 200 penalty units—$22,000 for an individual and $110,000 for a company—to 2,000 penalty units, which is $220,000 for an individual and $1.1 million for a company. For serious and repeated breaches of privacy, the penalty will be 2,000 penalty units. This is another remedy for consumers and will encourage compliance with the Privacy Act.[60]

1.29 The interaction between civil and criminal proceedings is addressed in proposed Division 3 of new Part VIB of the Privacy Act.[61]

Amendment of other Commonwealth Acts

1.30 Schedule 5 of the Bill contains consequential amendments to Commonwealth Acts, other than the Privacy Act. The EM states that these amendments primarily replace references to the Information Privacy Principles or National Privacy Principles with the APPs, and insert new definitions, including certain credit reporting terms, into Commonwealth Acts which interact with the Privacy Act.[62]

---

55 Proposed new subsections 5B(2) and 5B(3) of the Privacy Act; items 4 and 6 of Schedule 4 of the Bill.

56 Item 189 of Schedule 4 of the Bill.

57 Proposed new section 80V of the Privacy Act; item 189 of Schedule 4 of the Bill.

58 Proposed new section 80W of the Privacy Act; item 189 of Schedule 4 of the Bill.

59 Proposed new section 13G of the Privacy Act; item 50 of Schedule 4 of the Bill.

60 *House of Representatives Hansard*, 23 May 2012, p. 5211.

61 Item 189 of Schedule 4 of the Bill.

62 EM, p. 5.

Application, transitional and savings provisions

1.31 Schedule 6 of the Bill addresses transitional issues relating to the commencement of the Bill's substantive provisions.[63] In her second reading speech, the Attorney-General noted that there will be a nine-month transition period in which industry and government agencies are to review and update their privacy policies and practices.[64]

Financial and Regulation Impact Statements

1.32 The EM states that the Bill will have no significant impact on Commonwealth expenditure or revenue. However, a Regulation Impact Statement is required for the credit reporting measures contained in the Bill.[65]

Conduct of the inquiry

1.33 Details of the inquiry, the Bill and associated documents were placed on the committee's website at http://www.aph.gov.au/senate_legalcon. The committee also wrote to 117 organisations and individuals, inviting submissions by 9 July 2012. Submissions continued to be accepted after that date.

1.34 The committee received 59 submissions, which are listed at Appendix 2. Public submissions are available on the committee's website.

1.35 The committee held public hearings at Parliament House in Canberra on 10 and 21 August 2012. A list of the witnesses who appeared at the hearings is at Appendix 3, and the *Hansard* transcripts are available through the committee's website.

Acknowledgement

1.36 The committee thanks those organisations and individuals who made submissions and gave evidence at the public hearing.

Scope of this report

1.37 The committee's report is structured in the following way: chapter 2 examines some of the key issues raised during the committee's inquiry in relation to the APPs; chapters 3 and 4 discuss some of the proposed credit reporting definitions and proposed provisions for the regulation of credit reporting; chapter 5 examines issues raised with respect to the powers and functions of the Commissioner, as well as the proposed civil penalty regime; and chapter 6 contains the committee's views and recommendations.

---

63 EM, p. 5.

64 *House of Representatives Hansard*, 23 May 2012, p. 5212.

65 EM, p. 5. The Regulation Impact Statement appears at pp 6-43 of the EM.

Notes on references

1.38 References to the committee *Hansard* are to the proof *Hansard*. Page numbers may vary between the proof and the official *Hansard* transcript.

CHAPTER 2

Australian Privacy Principles

2.1 One of the major reforms in the Bill is the creation of the Australian Privacy Principles (APP). The APPs replace the Information Privacy Principles (IPPs) – which apply to Commonwealth government agencies – and the National Privacy Principles (NPPs) – which apply to some private sector organisations. The APPs will apply to Commonwealth government agencies and private sector organisations (to be referred to jointly as 'APP entities' in this report); however, the APPs do not necessarily apply uniformly to Commonwealth government agencies and private sector organisations.[1]

2.2 There are thirteen proposed APPs, covering the following matters:

- APP 1 – open and transparent management of personal information;
- APP 2 – anonymity and pseudonymity;
- APP 3 – collection of solicited personal information;
- APP 4 – dealing with unsolicited personal information;
- APP 5 – notification of the collection of personal information;
- APP 6 – use or disclosure of personal information;
- APP 7 – direct marketing;
- APP 8 – cross-border disclosure of personal information;
- APP 9 – adoption, use or disclosure of government-related identifiers;
- APP 10 – quality of personal information;
- APP 11 – security of personal information;
- APP 12 – access to personal information; and
- APP 13 – correction of personal information.[2]

2.3 During the inquiry, a representative from the Attorney-General's Department (Department) informed the committee that the APPs are 'broadly based' on the NPPs, but there are several new features included in the APPs:

> Firstly, there are new, discrete privacy principles about maintaining privacy policies [APP 1]…That is an enhanced obligation for agencies and organisations to say publicly to their customers and to citizens: 'This is how

1 For example, APP 7 and APP 8 apply only to private sector organisations. The Attorney-General's Department explains that this distinction is due to the organisation-specific activities of private sector organisations: see answer to question on notice, received 3 September 2012, p. 1.

2 Item 104 of Schedule 1 of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Bill).

> we collect, use and disclose information and these are the things that you could anticipate we would do once we have your information.'
>
> There is also a new principle to deal with the unsolicited collection of personal information – that is, when personal information is provided to an organisation in an unsolicited way, so the organisation has not asked for it but they have received it…
>
> There is also a new separate principle dealing with direct marketing. The [NPPs] did deal with direct marketing previously, [however in the APPs the key issue] is around choice—the capacity of individuals to be able to opt out of receiving direct marketing information in different circumstances…
>
> Then there is a new principle, Australian Privacy Principle 8, which deals with the cross-border disclosure of personal information…What the principle says is that it is open to an organisation to transfer data overseas. It has to take some steps to make sure that the recipient of the data will not deal with it in a manner that would be inconsistent with the Australian Privacy Principles, and that is typically dealt with through contract. But then it says: if you do that, absent a number of other features, you, the disclosing entity, will remain accountable for anything that might happen to that data in the future.[3]

2.4 Although many submitters and witnesses expressed support for the proposed APPs, concerns were raised in relation to the complexity of the principles, issues relating to the practical operation of specific APPs (or aspects of specific APPs), and certain definitions and terms contained in the APPs. This chapter examines some of those issues and concerns.

Complexity of the APPs

2.5 In 2010-2011, the Senate Finance and Public Administration Legislation Committee (F&PA committee) inquired into an Exposure Draft of the Bill (F&PA inquiry).[4] One issue commented on by the F&PA committee was the complexity of the proposed privacy principles. The F&PA committee supported the need for clarity, simplicity and accessibility, and concluded that the proposed APPs could be improved:

> The committee recommends that the Department of the Prime Minister and Cabinet [which then had portfolio responsibility for privacy legislation] re-assess the draft Australian Privacy Principles with a view to improving

3 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, pp 2-3.

4 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011.

> clarity through the use of simpler and more concise terms and to avoid the repetition of requirements that are substantially similar.[5]

2.6 The Australian Government accepted this recommendation in principle, advising that it would consider options to improve overall clarity and, in particular, to avoid repetition throughout the principles.[6] In additional information provided to this committee during the current inquiry, the Department confirmed that the APPs have been restructured:

> The APPs generally have been restructured to shorten the length of the principles. This has been achieved by use of a table in [proposed new section] 16A of the Bill which captures the common permitted situations for the collection, use and disclosure of personal information. The use of the table has reduced repetition within the APPs.[7]

Australian Privacy Principle 2

2.7 Australian Privacy Principle 2 (APP 2) deals with anonymity and pseudonymity. This principle gives an individual the right not to identify him or herself, or to use a pseudonym, when dealing with an APP entity in relation to a particular matter. The right does not apply in certain circumstances – namely, where an APP entity is required or authorised by law to deal with individuals who have identified themselves, or where it is impracticable for the APP entity to deal with individuals who have not identified themselves.[8]

'Impracticable' to deal with unidentified individuals

2.8 Facebook, Google, IAB and Yahoo!7 argued that the wording of APP 2.2(b) – which provides an exemption for APP entities where 'it is impracticable for the APP entity to deal with individuals who have not identified themselves' – does not address the issue of pseudonymity. The joint submission suggested that APP 2.2(b) should refer to 'individuals who have not identified themselves or who use a pseudonym' to ensure that this scenario is specifically covered in the exemption.[9]

2.9 Further, Facebook, Google, IAB and Yahoo!7 submitted that the EM to the Bill should outline further examples of when APP entities may find it 'impracticable' to deal with individuals on an anonymous or pseudonymous basis, such as:

---

5 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 18 (Recommendation 1).

6 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 3.

7 Additional information, received 3 September 2012, p. 1.

8 APP 2.1-APP 2.2.

9 *Submission 39*, pp 2-3.

- opt-in services that rely on a real name culture to help people find and connect with each other, and to promote user safety and security (for example, Facebook); and
- organisations operating e-commerce websites where there is a need for users to authenticate their identity through the use of credit cards.[10]

Departmental response

2.10 The Department noted that the right contained in APP 2 is not absolute. For example, under APP 2.2(b) – if it is impracticable for an entity to offer the option of a pseudonym unless the entity obtains identification details from the individual – the entity is not required to provide that option. Further:

> The suggestion put forward by some submitters is that clarity could be enhanced in this exception if it specifically referred to the impracticality of providing a pseudonym. The Government is considering options to enhance clarity around the application of this exception.[11]

Australian Privacy Principle 3

2.11 Australian Privacy Principle 3 (APP 3) deals with the collection of solicited personal information. The principle prohibits an APP entity from collecting personal information (other than sensitive information) unless the information is 'reasonably necessary' for one or more of the entity's functions or activities (APP 3.1). In the case of a Commonwealth agency, the information can also be 'directly related to' one or more of the entity's functions or activities. The principle allows for the collection of sensitive information in certain circumstances.[12]

2.12 Several submitters raised concerns regarding APP 3 with views expressed on a range of issues, including the breadth of the principle; 'consent' for the collection of sensitive personal information; and the means of collecting personal information.

Breadth of APP 3

2.13 The Law Institute of Victoria (LIV) argued that the phrase 'reasonably necessary for, or directly related to, one or more of the entity's functions or activities' is too broad:

> [T]he construction of APP [3.1] allows multi-function entities to request personal information that is not directly related to the goods or services actually requested by an individual, so long as the information is reasonably necessary for one or more of the entity's functions. The LIV is concerned that APP [3.1] might enable entities to make the provision of goods and

10 *Submission 39*, p. 3.

11 Answer to question on notice, received 3 September 2012, p. 4.

12 APP 3.1-APP 3.4.

> services conditional upon irrelevant and potentially unnecessary personal information being provided by an individual.[13]

2.14 The LIV argued further that APP 3.1 contains a unilateral test, which focuses on the entity and not on the individual:

> The test permits the collection of personal information for any of the entity's purposes, even if the individual has transacted in respect of a confined, limited function or activity. The LIV recommends that this test, wherever appearing, should be amended to 'reasonably necessary for the function or activity in which the individual is engaging' or similar.[14]

2.15 The NSW Department of Attorney General and Justice similarly referred to the broad ability of Commonwealth agencies to collect information in accordance with the 'directly related to' test:

> Under APP 3.1 the only nexus required for collection is that the information is directly related to an activity of the agency, not that the collection would be necessary for (or even assist) that activity. If it is not necessary for an entity to collect information in order to perform its activities it is questionable why it should be entitled to do so.[15]

2.16 More broadly, the Law Council and the NSW Privacy Commissioner considered that Commonwealth agencies and private sector organisations should be subject to the same obligations regarding the collection of personal information. In their view, APP 3 should be amended to remove the exception for a government agency to collect information that is 'directly related to' one or more of its functions.[16]

Evidence to the F&PA committee's inquiry and government response

2.17 During its 2010-2011 inquiry, the F&PA committee heard arguments regarding use of the term 'reasonably necessary for, or directly related to' in APP 3 and made a recommendation based on its findings:

> The committee recommends that in relation to the collection of solicited information principle (APP 3), further consideration be given to:
>
> - whether the addition of the word 'reasonably' in the 'necessary' test weakens the principle; and
>
> - excluding organisations from the application of the 'directly related to' test to ensure that privacy protections are not compromised.[17]

---

13 *Submission 8*, Attachment 1, pp 4-5.

14 *Submission 8*, p. 2.

15 *Submission 55*, p. 6.

16 *Submission 14*, p. 6 and *Submission 42*, p. 5, respectively.

17 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 72 (Recommendation 8).

2.18 In response to the F&PA inquiry, the Australian Government reiterated its support for use of the 'reasonably necessary' test in APP 3:

> The requirement on entities to collect only personal information that is reasonably necessary to their functions, requires the collection of personal information to be justifiable on objective grounds, rather than on the subjective views of the entity itself. This is intended to expressly clarify that the test is objective (rather than implied) and to enhance privacy protection. Making it clear that the necessity of the collection must be reasonable is intended to reduce instances of inappropriate collection of personal information by entities.[18]

2.19 In relation to the 'directly related to' test, the government agreed to reconsider the application of the test to private sector organisations[19] and the test has now been removed from the Bill in relation to APP entities which are organisations.

2.20 The Department informed the committee:

> There has been careful consideration given to the inclusion and breadth of agency specific provisions in the proposed APPs. While the general approach has been to apply the single set of principles to all entities, in some cases there is a clear rationale for applying separate rules.[20]

2.21 In relation to the 'directly related to' test in APP 3, the Department appears to have accepted the F&PA committee's view that the 'reasonably necessary' test 'provides organisations with sufficient flexibility, and is, in fact substantially similar to what is now provided in NPP 1'.[21]

Departmental response in the current inquiry

2.22 In the current inquiry, the Department again responded to broad concerns regarding the use of the term 'reasonably necessary' in the Bill. The Department affirmed its support for the inclusion of a 'reasonably necessary' standard in each circumstance in which that standard appears in the Bill. Two reasons were given in support of this position:

- the concepts of 'reasonably necessary' and 'necessary' coexist in the Privacy Act without any confusion or compromise on privacy protection; and

---

18 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 3.

19 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 3.

20 Answer to question on notice, received 3 September 2012, p. 1.

21 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 72. NPP 1 relates to the collection of personal information by private sector organisations.

- the Privacy Act recognises that there are instances where an objective element applies to an activity where the 'necessary' formulation appears.[22]

2.23 The Department informed the committee:

> The general approach taken in the Bill reinforces this current approach from the Act. First, the 'reasonably necessary' formulation is used in APPs 3, 6, 7 and 8, and exceptions listed in [proposed new section] 16A, to provide clarity that an objective test applies in relation to each of those activities. Secondly, where the 'necessary' formulation is used on its own, the addition of 'reasonably' is not required because it [is] preceded by a 'reasonably believes' test (see, for example, items 1, 2, 3, 6, and 7 in table in [proposed new section] 16A).[23]

2.24 The 'directly related to' test is a current feature of IPP 1.1[24] in relation to Commonwealth agencies. The Department stated that this feature is being retained in APP 3, not only to ensure flexibility in the requirements of APP entities but also:

> …because there may be agencies (less so for organisations) that need to collect personal information to effectively carry out defined functions or activities but who may not meet an objective 'reasonably necessary' test.[25]

'Consent' for the collection of sensitive personal information

2.25 APP 3.3 prohibits an agency from collecting sensitive information about an individual without the individual's 'consent', unless one of the exceptions in APP 3.4 applies.[26] Current subsection 6(1) of the Privacy Act defines 'consent' to mean 'express

22 Additional information, received 29 August 2012, p. 3.

23 Additional information, received 29 August 2012, p. 3. The Attorney-General's Department noted that a dual 'reasonably believes' and 'reasonably necessary test' applies in relation to enforcement body and enforcement related activity exceptions due to their being based on NPP 2.1(h). NPP 2.1(h) allows for the use and disclosure of personal information where an organisation reasonably believes that the use or disclosure is reasonably necessary for certain law enforcement activities by an enforcement body.

24 IPP 1 relates to the manner and purpose of collection of personal information by Commonwealth agencies.

25 Answer to question on notice, received 3 September 2012, p. 5. It was further noted that agencies are subject to stricter oversight and accountability arrangements through Parliament, the Executive and the Commonwealth Ombudsman.

26 These exceptions include: where collection is required or authorised under an Australian law or court order; where a permitted general situation or permitted health situation exists; certain circumstances relating to law enforcement; and where the entity is a non-profit organisation and the information relates only to the organisation's activities and solely to the members of the organisation.

consent or implied consent', and the EM notes that this meaning is being retained in the Bill.[27]

2.26 The NSW Privacy Commissioner submitted that it is not appropriate to rely on implied consent in relation to the collection of sensitive information, and that APP 3.3 should be amended to require express consent only.[28]

Consideration of the meaning of consent and government response

2.27 In its 2008 report, the Australian Law Reform Commission (ALRC) considered the meaning of 'consent' as it applies to the privacy principles. The ALRC concluded that the most appropriate way to clarify the meaning of this term would be for the Office of the Privacy Commissioner (now the Office of the Australian Information Commissioner (OAIC)) to provide guidance in this regard:

> **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'. [29]

2.28 The Australian Government accepted this recommendation, noting that the decision to provide guidance is a matter for the Australian Privacy Commissioner.[30] The F&PA committee also supported ALRC Recommendation 19-1 and called on the OAIC to prioritise consideration of the matter to ensure that appropriate guidance is available concurrently with the implementation of the new legislation.[31] The

---

27 Explanatory Memorandum (EM), p. 54. Also see the Australian Privacy Foundation, which argued that the definition of consent in the Privacy Act should be amended to prevent the term being interpreted in such a way that it undermines the APPs: *Submission 49*, p. 9; and the Law Institute of Victoria, which argued that the current definition of consent does not preclude consent unreasonably obtained or obtained in a way which undermines the objectives or purpose of the APPs: see *Submission 8*, p. 2.

28 *Submission 42*, p. 6.

29 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Volume 1, p. 686.

30 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, p. 38.

31 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 33 (Recommendation 4).

Australian Government's position has not changed since its response to the ALRC's recommendation.[32]

Australian Privacy Principle 5

2.29 Australian Privacy Principle 5 (APP 5) deals with notification of the collection of personal information. At or before the time of collection or, if that is not practicable, as soon as practicable afterward, an APP entity must take such steps (if any) as are reasonable in the circumstances to notify an individual of certain matters set out in APP 5.2: for example, whether the entity is likely to disclose the personal information to overseas recipients (APP 5.2(i)); and, if so, the countries in which such recipients are likely to be located, if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them (APP5.2(j)).

Notification requirements

2.30 Some submitters expressed concerns about the clarity of the principle and implementation of the notification requirement. For example, the Australian Broadcasting Corporation (ABC) submitted that there is insufficient guidance on the meaning of what is reasonable in any given set of circumstances.[33] The Australian Bankers' Association (ABA) commented that the notification requirement is impractical because banks collect personal information from agencies 'on a regular basis about the hundreds of thousands of individuals on behalf of whom they execute international transfer payments'.[34]

2.31 One of the notification matters listed in APP 5.2 is:

> (c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection).

2.32 The Australian Finance Conference (AFC) submitted that the obligation in APP 5.2(c) to notify an individual of the name of the Australian law on which the collection is based creates a potentially unnecessary compliance obligation, particularly for organisations in the financial services sector operating under a 'significant range of laws which may provide a permitted basis for collection of personal information'.[35] The AFC recommended eliminating the statutory obligation

---

32 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 5; and answer to question on notice, received 3 September 2012, p. 2.

33 *Submission 19*, p. 2.

34 *Submission 24*, pp 9-10.

35 *Submission 36*, p. 5.

and allowing entities to specify the relevant law where doing so is reasonable in the circumstances.[36]

Australian Privacy Principle 6

2.33 Australian Privacy Principle 6 (APP 6) deals with the use or disclosure of personal information. If an APP entity holds personal information about an individual that was collected for a particular purpose (the 'primary purpose'), the entity must not use or disclose the information for another purpose (the 'secondary purpose') unless they have the individual's consent, or the circumstances set out in APP 6.2 or APP 6.3 apply (APP 6.1).

General exception

2.34 APP 6.2 creates an exception to the general rule in APP 6.1, allowing an APP entity to disclose personal information in certain circumstances. The EM summarises these circumstances:

> [T]here are a number of exceptions enabling the use or disclosure of personal and sensitive information where required or authorised by or under Australian law or a court/tribunal order; in permitted general situations ([proposed new] section 16A); in permitted health situations ([proposed new] section 16B); and where an 'APP entity reasonably believes that the use of disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body'. The final exception is aimed at enabling any APP entity to cooperate with an enforcement body where it may have personal information relevant to an enforcement related activity of that enforcement body.[37]

2.35 The Office of the Victorian Privacy Commissioner expressed concern at the complexity of APP 6 and considered the division between APP 6.1 and APP 6.2 to be unnecessary.[38] The Australian Privacy Foundation (Privacy Foundation) similarly argued that splitting the provisions across APP 6.1 to APP 6.3 is misleading:

> It is not clear why this has been done and it is potentially confusing and misleading. Sub-section (1) is not only meaningless without an understanding that 6.2 and 6.3 contains 'exceptions' to consent, but is actively misleading in that it implies that consent has a much more prominent role than it does in reality…APP 6 needs to be rewritten so as not to be confusing and misleading. Consent should be only one of a number of conditions for use and disclosure, with all exceptions in a single clause, so as to give a much more realistic impression of the effect of the law.[39]

---

36 *Submission 36*, p. 5.

37 EM, p. 80.

38 *Submission 17*, p. 8.

39 *Submission 49*, p. 15.

Biometric information and biometric templates exception

2.36 APP 6.3 also creates an exception to the general rule in APP 6.1, allowing a Commonwealth agency to disclose personal information if:

> (a) the agency is not an enforcement body; and
>
> (b) the information is biometric information or biometric templates; and
>
> (c) the recipient of the information is an enforcement body; and
>
> (d) the disclosure is conducted in accordance with the guidelines made by the [Australian Information] Commissioner for the purposes of this paragraph.

2.37 The OAIC considered APP 6.3 to be unnecessary. Its submission noted APP 6.2(e), which provides an exception where an APP entity reasonably believes that the use or disclosure of information is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, an enforcement body.[40]

2.38 Liberty Victoria also did not support APP 6.3, arguing that the ability of an enforcement body to collect information without an individual's permission from a non-enforcement agency is disproportionate and has the potential for serious abuse:

> It would damage the community's trust in non-enforcement agencies because they would be perceived as being, and would become, the agents of enforcement agencies. In relation to the provision of medical services and biometric data, the invasive consequences will be grave. Liberty Victoria submits that the proposed provision should be removed.[41]

Departmental response

2.39 In relation to the comments of the OAIC, the Department advised that APP 6.3 is intended to allow non-law enforcement agencies to disclose biometric information and templates for a secondary purpose to enforcement bodies where an APP 6 exception, including the enforcement related activity exception in AAP 6.2(e), is not applicable:

> This may occur where the disclosure is for purposes such as identity/nationality verification or general traveller risk assessment, in circumstances where there is a legitimate basis for the disclosure but no criminal enforcement action is on foot…The policy rationale in APP 6.3 recognises that non-law enforcement agencies have current, and will have future, legitimate reasons to disclose biometric information and templates to enforcement bodies, but that this should occur within a framework that protects against improper disclosure.[42]

---

40 *Submission 47,* p. 19.

41 *Submission 13,* p. 5.

42 Answer to question on notice, received 3 September 2012, pp. 7-8. The answer notes that additional safeguards are provided for throughout the Bill, including oversight by the Australian Privacy Commissioner.

Australian Privacy Principle 7

2.40 Australian Privacy Principle 7 (APP 7) deals with direct marketing. The principle prohibits a private sector organisation which holds personal information about an individual from using or disclosing the information for the purpose of direct marketing (direct marketing prohibition) (APP 7.1). There are some exceptions to this prohibition, relating to: personal information other than sensitive information; sensitive information; and organisations which are contracted service providers.[43]

2.41 Some submissions did not support APP 7 at all. For example:

- the Australian Direct Marketing Association (ADMA) argued that principles-based legislation should not include a specific marketing provision such as APP 7;[44]
- the Australian Industry Group considered that APP 7 would seriously impede the ability of businesses to market and sell their products and services;[45] and
- the Privacy Foundation recommended that APP 7 should also apply to Commonwealth agencies as 'the boundaries between private and public sectors are becoming increasingly blurred, and government agencies are now commonly undertaking direct marketing activities'.[46]

2.42 Some stakeholders expressed concern in relation to particular aspects of APP 7, including: the subheading to APP 7.1 and general structure of APP 7; exceptions to the general prohibition in APP 7.1; and the opt-out mechanisms in APP 7.

Subheading to APP 7.1 and general structure of APP 7

2.43 Several stakeholders commented on the heading to APP 7.1, that is, 'Prohibition on direct marketing'. ADMA, for example, argued that this is confusing for consumers, businesses and marketing suppliers as:

> [APP 7] is not, in effect, a prohibition. Instead the provision permits direct marketing under certain defined conditions. Therefore, the term "prohibition" should be removed.[47]

---

43 APP 7.2–APP 7.5.

44 *Submission 7*, p. 5.

45 *Submission 16*, p. 1.

46 *Submission 49*, pp 16.

47 *Submission 7*, p. 2. For similar comments, also see: Foxtel, *Submission 21*, pp 3-4; Acxiom Australia, *Submission 32*, p. 1; Kimberly-Clark Australia, *Submission 46*, p. 1.

2.44 The Fundraising Institute of Australia (FIA) submitted that charitable fundraising depends on direct marketing techniques and the way in which the subheading is drafted will cause confusion and distress in the fundraising community, particularly among smaller charities:

> FIA is already receiving calls from members worried about their ability to continue their normal fundraising activities utilising direct marketing methods.[48]

2.45 ADMA supported the 'more practical, clear, positive drafting' in the Exposure Draft of the Bill (which contained the subheading 'Direct marketing'),[49] whereas the Law Council submitted that APP 7, if it is to be retained, should be restructured along the same lines as APP 6:

> The structure of APP 7 is a blanket prohibition on direct marketing, followed by a list of exceptions under which direct marketing is permitted. The structure of APP 6 is to prohibit use and disclosure of personal information unless certain circumstances apply…[T]he structure of APP 7 suggests that direct marketing is generally prohibited unless an exception applies, whereas the structure of APP 6 is such that use and disclosure in certain situations is permitted and in all other cases it is prohibited.[50]

Departmental response

2.46 In 2011, the F&PA committee recommended that the drafting of APP 7 should be reconsidered with the aim of improving its structure and clarity. The intent of this recommendation was to ensure that the principle is not undermined.[51] The Australian Government accepted this recommendation in principle, advising that it would consider options to improve clarity and structure.[52]

2.47 During the current inquiry, the Department informed the committee that it had adopted the approach evident in the Bill following the recommendation of the F&PA committee.[53] Further:

> The approach in [APP 7] of casting the principle as a 'prohibition' against certain activity followed by exceptions is a drafting approach used in principles-based privacy regulation to clearly identify the information-

---

48 *Submission 4*, p. 2. Also see Salmat, which argued that the confusion could lead to a significant increase in consumer complaints on the mistaken assumption that direct marketing is prohibited (when in fact it is not): *Submission 26*, p. 8.

49 *Submission 7*, p. 6. Also see section 8 of the Exposure Draft Bill.

50 *Submission 14*, p. 10.

51 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 142 (Recommendation 10).

52 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 8.

53 Answer to question on notice, received 3 September 2012, p. 8.

> handling activity that breaches privacy, followed by any exceptions to this general rule that would permit an entity to undertake the activity. This is consistent with the practical effect of the current [IPPs] and the [NPPs]. For example, both IPP 1 and NPP 1 begin by expressly stating that the collection of personal information is not permitted unless certain exceptions apply.[54]

Exceptions to the general prohibition in APP 7.1

2.48 APP 7.2 allows the use or disclosure of personal information (other than sensitive information) for the purpose of direct marketing in certain circumstances. For example, one condition is that an individual 'would reasonably expect the organisation to use or disclose the information for that purpose' (APP 7.2(b)). Foxtel submitted that very little guidance is given regarding the assessment of a reasonable expectation and called for further clarification on this issue.[55]

2.49 APP 7.3(a) also allows for the use or disclosure of personal information (other than sensitive information) for the purpose of direct marketing in certain circumstances, including where the information is collected from someone other than the individual (APP 7.3(a)(ii)). The Queensland Law Society argued that APP 7.1 should contain a similar allowance to accommodate information which has been self-generated or developed by an organisation.[56]

2.50 APP 7.4 permits an organisation to use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose. The Privacy Foundation asserted that APP 7.4 should be strengthened with a requirement for express consent:

> …otherwise organisations will be free to use small print in terms and conditions, and 'bundled consent' to allow them to direct market using sensitive information.[57]

Opt-out mechanisms in APP 7

2.51 APP 7.2(c) and APP 7.3(c) require an organisation to provide a simple means by which an individual may easily request not to receive direct marketing communications from an organisation, if the organisation is to utilise the exceptions provided in APP 7.2 or APP 7.3.

2.52 APP 7.3 differs from APP 7.2 in that it includes situations where an individual 'would not reasonably expect the organisation to use or disclose the information' for direct marketing (APP 7.3(a)(i)). APP 7.3(d) therefore contains an additional safeguard: that in each direct marketing communication with the individual, the organisation must include a prominent statement that the individual may request not to

---

54 Additional information, received 29 August 2012, p. 1.

55 *Submission 21*, p. 4.

56 *Submission 3*, pp 1-2.

57 *Submission 49*, p. 18.

receive direct marketing communications, or otherwise draw the individual's attention to the fact that they may make such a request.

2.53 In addition, APP 7.6 explicitly provides that if an organisation uses or discloses personal information about an individual for the purpose of direct marketing, or for facilitating direct marketing by other organisations, the individual may:

- request not to receive direct marketing communications from the first organisation;
- request the first organisation not to use or disclose the information for facilitating direct marketing by other organisations; and
- request the first organisation to provide its source of the information.

Strength of the opt-out mechanisms

2.54 Several submitters commented on the opt-out provisions in APP 7. These comments concerned the strength of the provisions, and their current and future application. The Privacy Foundation, for example, argued that the mechanisms are not strong enough to protect consumers:

> APP 7.2 and 7.3 and 7.6 appear to have the effect of requiring all organisations to *maintain a facility* to allow people to 'opt-out' of direct marketing, but only those covered by 7.3 have to do anything *to draw an individual's attention to it*, and even then not with any prescribed level of prominence. Under 7.2, if the individual would reasonably expect to receive marketing communications, they are not even required to be notified – this seems perverse and is a very weak provision.[58]

2.55 The Privacy Foundation considered that APP 7 should be strengthened and simplified, including by requiring notification of opt-out and related rights in every marketing communication, not just those covered by APP 7.3.[59] This view contrasted with the submissions and evidence received from industry stakeholders.

Current and future application

2.56 Facebook, Google, IAB Australia and Yahoo!7 argued that, as there is no clear definition of 'direct marketing' in the Privacy Act, the wording of APP 7.2 and APP 7.3 means that individuals would be opting out of all direct marketing (such as advertisements), rather than just direct marketing which relies on the use or disclosure of their personal information:

> In the event that 'direct marketing' were interpreted to include advertisements, this would undermine advertising based business models, which is surely not the intention of the Proposed Law.
>
> We would like APP 7.2 and APP 7.3 to require an opt-out of direct marketing that relies on personal information. This will allow advertisements to still be served (not based on personal information).

58 *Submission 49*, p. 17 (with emphasis in the original).

59 *Submission 49*, p. 17.

> This is particularly important where the advertisements are part of a service that is free to access and ad-supported.[60]

2.57 The FIA also questioned the lack of clarity in APP 7.3, and submitted in particular that new social media technologies complicate the provision of opt-out details as envisaged under the proposed legislation.[61] ADMA agreed:

> The requirement to include an opt-out statement in each direct marketing communication is not possible with regard to all marketing and advertising channels due to space constraints. E.g. – online advertisements, banner ads, twitter feed etc. More compliance issues regarding this requirement will arise in the future as communication channels evolve and advance. This will give rise to many more examples where the inclusion of an opt-out is not possible due to the channel, technology or medium.[62]

2.58 ADMA submitted that 'APP 7.3(d) needs to be amended so that it can apply to every channel, is future proof and easy to apply across multiple technologies'.[63] Similarly, the FIA called for further consultation on the latest iteration of APP 7:

> There is clearly a case for further amendment to ensure that the Principle will apply in all circumstances, with provisions for specific channels being worked out with the Privacy Commissioner in codes and/or guidelines to ensure technological neutrality.[64]

2.59 Kimberly-Clark added that the requirement in APP 7.3(d) will: cause compliance difficulties; discourage the use of third party data cleansing and updating services; impact on the ability to communicate effectively with customers and provide the best possible products and services for clients' needs; and degrade the customer experience, which is critical to brand reputation.[65]

---

60 *Submission 39*, p. 6.

61 *Submission 4*, p. 2.

62 *Submission 7*, p. 7.

63 *Submission 7*, p. 7.

64 *Submission 4*, p. 2.

65 *Submission 46*, p. 2. Also see GEON, *Submission 37*, p. 1.

Departmental response

2.60 The F&PA committee recommended that the structure of APP 7.2 and APP 7.3 in relation to APP 7.3(a)(i) be reconsidered.[66] The Australian Government recognised the need to consider further simplification of these provisions and undertook to develop appropriate amendments to the draft legislation.[67]

2.61 In the Bill, APP 7 has been significantly restructured; however, the substantive provisions of APP 7.2 and APP 7.3 are largely unchanged. The Department addressed stakeholders' concerns regarding these provisions as follows.

2.62 In response to the concerns of Facebook, Google, IAB Australia and Yahoo!7, the Department assured the committee:

> APP 7 will not cover forms of direct marketing that are received by individuals that do not involve the use or disclosure of their personal information, such as where they are randomly targeted for generic advertising through a banner advertisement. Nor will APP 7 apply if it merely targets a particular internet address on an anonymous basis for direct marketing because of its web browsing history. These are current online direct marketing activities that will not be affected by the amendments.[68]

2.63 The Department noted that opt-out mechanisms are currently used for many types of online communication and rejected the notion that compliance with APP 7.3(d) will be unduly onerous or technically difficult:

> The opt out requirements are designed to operate flexibly so that organisations can develop an appropriate mechanism tailored to the particular form of advertising they are undertaking, while raising sufficient awareness amongst consumers of their right to opt out, and the means by which they can easily do so. While the Department notes that lengthy opt out messages may be impractical in some circumstances, there may be shorter messages (eg. 'opt-out' with a link) that could be considered.
>
> The principle will require organisations to adapt to new direct marketing rules that enhance the privacy protections of consumers. Shifting the balance more in favour of consumers may require an additional mechanism to be developed.[69]

---

66 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 150 (Recommendation 13).

67 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 9.

68 Additional information, received 29 August 2012, p. 2.

69 Additional information, received 29 August 2012, pp 2-3.

Australian Privacy Principle 8

2.64 Australian Privacy Principle 8 (APP 8) deals with the cross-border disclosure of personal information:

> 8.1 Before an APP entity discloses personal information about an individual to a person (the overseas recipient):
>
> (a) who is not in Australia or an external Territory; and
>
> (b) who is not the entity or the individual;
>
> the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

2.65 APP 8.2 sets out six exceptions to APP 8.1. For example, APP 8.1 does not apply to the disclosure of personal information about an individual by an APP entity if: the APP entity reasonably believes that the 'overseas recipient' is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the APPs protect the information, and there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme. (APP 8.2(a)).

2.66 APP 8 is supported by an accountability mechanism in proposed new section 16C of the Privacy Act (item 82 of Schedule 1 of the Bill). Under proposed new subsection 16C(2), if the section applies, an act done, or a practice engaged in, by an 'overseas recipient' in breach of the APPs is taken for the purposes of the Privacy Act:

- to have been done, or engaged in, by the relevant APP entity; and
- to be a breach of the relevant APPs by the APP entity.

2.67 The EM states:

> Section 16C is a key part of the Privacy Act's new approach to dealing with cross-border data flows. In general terms, there are currently two internationally accepted approaches to dealing with cross-border data flows: the adequacy approach, adopted by the European Union [EU] in the Data Protection Directive of 1996, and the accountability approach, adopted by the [Asia-Pacific Economic Cooperation] Privacy Framework in 2004. NPP 9 [the current privacy principle, which deals with transborder data flows] was expressly based on the adequacy approach of the EU Directive. Under the new reforms, APP 8 and section 16C will introduce an accountability approach more consistent with the [Asia-Pacific Economic Cooperation] Privacy Framework.
>
> The accountability concept in the [Asia-Pacific Economic Cooperation] Privacy Framework is, in turn, derived from the accountability principle from the [Organisation for Economic Co-operation and Development]

> Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980.[70]

General comments

2.68 Some submitters – such as the Law Institute of Victoria and Liberty Victoria – expressed support for APP 8,[71] whereas other stakeholders opposed the introduction of the principle. For example, Professor Graham Greenleaf from the Privacy Foundation told the committee:

> While it was a laudable aim to combine the NPPs and the IPPs and try to get one set of privacy standards across Australia, what we have ended up within the APPs is in fact a serious step backwards. On our detailed analysis…eight of the 13 principles are weaker than the NPPs or IPPs, so we have no advance. A number of them are very seriously defective. The most important of those is APP 8, concerning cross-border disclosures…While in theory imposing a liability on the exporter is a good idea, it is in our view an empty imposition of liability. The problem that the individuals concerned will have is how they prove on the balance of probability that any breach has occurred in some overseas destination, particularly when they do not even know where it is or the state of the laws in that particular country.[72]

2.69 The Law Council argued that APP 8 is too restrictive.[73] The Australian Finance Conference also raised a number of concerns with the provision:

> [A]s a matter of policy and drafting[,] APP 8 when combined with [proposed new section] 16C fails to achieve the key objectives of the Government (e.g. high level principles, simple, clear and easy to understand and apply) of the reforms. It also shifts the risk balance heavily to the entity and we query the individual interest justification to support that[.][74]

2.2 The majority of submissions and evidence focussed on three main issues with APP 8: its interaction with proposed new section 16C of the Privacy Act; breaches by 'overseas recipients' and inadvertent breaches; and the exceptions provided for in APP 8.2.

Interaction with proposed new section 16C

2.70 The NSW Privacy Commissioner commended the inclusion of proposed new section 16C in the Privacy Act,[75] but some other submitters questioned the appropriateness of the provision in view of the requirement in APP 8.1 for an

---

70 EM, p. 70.

71 *Submission 8*, p. 1 and *Submission 13*, p. 5, respectively.

72 *Committee Hansard*, 10 August 2012, pp 49-50.

73 *Submission 14*, p. 10.

74 *Submission 36*, p. 6.

75 *Submission 42*, p. 4.

APP entity to have taken 'such steps as are reasonable in the circumstances to ensure that the overseas recipient' did not breach the APPs.

2.71 Facebook, Google, IAB Australia and Yahoo!7 submitted:

> We wholeheartedly support requiring disclosing entities to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. However, we are concerned that an entity disclosing personal information about an individual to an overseas recipient is subject to strict liability (by virtue of section 16C(2) (Acts and practices of overseas recipients of personal information)) even if that entity took all reasonable steps to ensure that the overseas recipient complies with the APPs.
>
> An APP entity disclosing personal information about an individual to an overseas recipient, that discharges an onus of establishing that it took all reasonable steps to ensure that the overseas recipient complies with the APPs, should thereby make out a defence to liability pursuant to APP 8.1.[76]

2.72 The question of what will constitute reasonable steps in the 'cloud environment'[77] concerned the Queensland Law Society. Its submission suggested that 'the pivot point should be moved back a notch to reflect what reasonable entities do in like situations'.[78] ADMA agreed that the implications of APP 8 should be reassessed due to the increasing prevalence of cloud computing.[79]

2.73 According to the EM:

> In practice, the concept of taking 'such steps as are reasonable in the circumstances' will normally require an entity to enter into a contractual relationship with the overseas recipient.[80]

2.74 In view of this, the NSW Privacy Commissioner argued that APP 8.1 should be amended to require an APP entity to enter into a contractual relationship with an 'overseas recipient', unless that would not be reasonable in the circumstances.[81]

---

76 *Submission 39*, pp 6-7. Facebook, Google, IAB Australia and Yahoo!7 alternatively suggested that the Australian Information Commissioner issue guidelines regarding what matters will be considered in the assessment of an APP 8 breach: see answer to question on notice, received 23 August 2012, p. 2. Also see Law Council of Australia, *Submission 14*, p. 11; Australian Bankers' Association, *Submission 24*, p. 11.

77 'Cloud environment' is a technical term for the practice of using a network of remote servers hosted on the Internet to store, manage and process data, rather than a local server: see http://computer.howstuffworks.com/cloud-computing/cloud-computing.htm (accessed 2 September 2012).

78 *Submission 3*, p. 2.

79 *Submission 7*, p. 3.

80 EM, p. 83.

81 *Submission 42*, p. 7. If not reasonable in the circumstances, the NSW Privacy Commissioner recommended that an entity could take other reasonable steps.

The Privacy Foundation also suggested that the Australian Information Commissioner (Commissioner) should be required to issue guidelines concerning model clauses, or a model contract, for these purposes.[82]

Evidence to the F&PA committee's inquiry and government response

2.75 The F&PA committee directly addressed the suggestion that the OAIC should issue guidelines on the application of APP 8, recommending:

> …that the Office of the Australian Information Commissioner develop guidance on the types of contractual arrangements required to comply with APP 8 and that guidance be available concurrently with the new Privacy Act.[83]

2.76 The Australian Government supported this recommendation, noting that it is consistent with the government's response to ALRC Recommendation 31-7[84] (which also recommended that the OAIC develop and publish guidance on the Cross-border Data Flows principle, including 'the issues that should be addressed as part of a contractual agreement with an overseas recipient of personal information').[85]

Breaches by overseas recipients

2.77 A few submitters questioned the position whereby local law requires an 'overseas recipient' to use or disclose personal information which it has received from an APP entity subject to the Privacy Act. Min-it Software submitted that the Bill should provide further clarification regarding the liability of an APP entity in this scenario.[86]

2.78 In evidence at the first public hearing, a departmental representative acknowledged the complex issue of conflict of laws between jurisdictions:

> The challenge comes when you are in Australia and you are seeking to comply with an overseas law that purports to bind you in Australia. We do not have a solution for that, primarily because allowing that to be an exception in the privacy law for Australia means that the content of Australian privacy law is effectively determined by every other country and

82 *Supplementary Submission 49*, p. 1.

83 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 176 (Recommendation 16).

84 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 10.

85 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, p. 48. Also see 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, p. 80.

86 *Submission 48*, p. 6.

> the laws that they purport to apply to Australian businesses. That is a great challenge in conflict of law but one that is not yet resolved.[87]

Inadvertent breaches

2.79 In relation to inadvertent disclosures, Kimberly-Clark Australia argued that there are instances where 'data may be subject to actions or attacks outside of [an entity's] control such as operational failure, fraud, sabotage and hacking and these must be taken into consideration before imposing liability'.[88] Foxtel agreed:

> [We] remain concerned that where an organisation takes such reasonable steps, including reviewing its security controls and protocols, the accountability provisions may still apply even where access to the relevant information is unauthorised, such as by hacking. Foxtel submits that the EM should provide further guidance to exclude this sort of 'disclosure' from falling within the new accountability regime in APP 8.[89]

2.80 Salmat suggested:

> It is important that the offence provisions apply only in the case of recklessness or intentional disregard for the privacy of an individual. That is, if a company has all the systems, procedures and practices in place to adequately protect the personal information of an individual, then it should not be disproportionately punished when an unintentional error occurs.[90]

2.81 An exception for inadvertent disclosures was not supported by the Department, whose response to these concerns emphasised the potentially significant consequences for affected individuals, as well as the potential for the inadvertent disclosure to highlight failures in the 'overseas recipients' security systems or personal information-handling protocols:

> These are matters that can be taken into account in an OAIC determination, or by a court if the matter was being considered in relation to a possible civil penalty for the Australian entity.[91]

2.82 Similarly, the Department did not countenance an exception for situations in which an 'overseas recipient' recklessly or intentionally performs an act or practice that has led to a breach of an individual's personal information:

> In such circumstances, the overseas recipient may not be readily subject to the jurisdiction of the OAIC or an Australian court. Again, while the actions of an overseas recipient may be taken into account in an OAIC determination or by a court if the matter was being considered in relation to

---

87 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, pp 5-6.

88 *Submission 46*, p. 3.

89 *Submission 21*, p. 6.

90 *Submission 26*, p. 6.

91 Additional information, received 29 August 2012, p. 13.

> a possible civil penalty for the Australian entity, the Government does not consider that this is sufficient reason to transfer accountability to the foreign recipient.[92]

APP 8.2 exceptions

2.83 Submitters commented on several of the exceptions to the application of APP 8 that are provided for in APP 8.2 and, in particular, the following exceptions set out in paragraphs APP 8.2(a), APP 8.2(b) and APP 8.2(e). APP 8.1 will not apply to the disclosure of personal information by an APP entity to an 'overseas recipient' if:

> (a) the entity reasonably believes that:
>
> > (i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and
> >
> > (ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
>
> (b) both of the following apply:
>
> > (i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;
> >
> > (ii) after being so informed, the individual consents to the disclosure; or
>
> …
>
> (e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party[.]

Substantially similar protections overseas

2.84 Facebook, Google, IAB Australia and Yahoo!7 contended that APP 8.2(a) does not have the intended effect of enabling individuals to take action through the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Enforcement Arrangement, or through other arrangements made between privacy regulators in different countries. Their submission called for APP 8.2(a)(ii) to be amended to explicitly ensure that these avenues of recourse can be pursued.[93]

2.85 The Privacy Foundation also remarked on APP 8.2(a), submitting that the threshold for this exemption – 'reasonable belief' on the part of the APP entity – is too weak and that only overseas privacy regimes approved by the Commissioner should qualify for this exception:

> [T]his is [a] completely unacceptable basis for allowing cross border transfers. Some organisations will inevitably make self-serving judgements

92 Additional information, received 29 August 2012, p. 14.

93 *Submission 39*, pp 7-8.

> about the level of protection in other jurisdictions and/or pay for advice that supports their desire to transfer…The only practical approach to remedying this defect in the current Bill is simply to delete 'the entity reasonably believes that', so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal…It would be preferabl[e] if there could be some prior considered assessment of similarity or adequacy by experts, such as the Privacy Commissioner, and this could be achieved by guidelines under the current Act.[94]

Informed consent to the disclosure

2.86 The OAIC expressed concern that the accountability mechanism in APP 8.1 and proposed new section 16C of the Privacy Act could be 'displaced' by APP 8.2(b). In that situation, individuals might not be able to access remedies if their information is mishandled by an 'overseas recipient'.[95] In recommending that APP 8.2(b) be removed from the Bill, the OAIC submitted:

> [I]n many cases there may be little real "choice" for an individual but to consent to their information being handled in that way. Once an individual does provide their consent, in many circumstances they are in effect abrogating any ability to seek redress for any mishandling by the overseas recipient.[96]

2.87 The NSW Privacy Commissioner warned similarly:

> [E]ntities might include this notification requirement in general privacy policies or other legal documents. Individuals may then 'agree' to something which may be buried in the middle of a privacy policy or legal document and may be drafted in complicated language, rather than plain English.[97]

2.88 Accordingly, the NSW Privacy Commissioner recommended the preparation of a template, setting out the form of notification that an APP entity must give for the purposes of APP 8.2. The NSW Privacy Commissioner also suggested that APP 8.2(b) should specify that an entity must notify the individual of the practical effect and potential consequences of APP 8.1 not applying to a disclosure of personal information to an 'overseas recipient'.[98]

---

94 *Submission 49*, p. 19.

95 *Supplementary Submission*, pp 1-2. For similar comments, also see Australian Privacy Foundation, *Submission 49*, p. 18.

96 *Supplementary Submission*, p. 2.

97 *Submission 42*, p. 8.

98 *Submission 42*, p. 8. Also see the Australian Privacy Foundation, which endorsed this proposal: *Submission 49*, p. 19.

2.89 In answer to a question on notice, the Department informed the committee that individuals have the right to complain about an act or practice that might breach the APPs,[99] and through the Commissioner obtain access to an enforceable remedy:

> Investigation of complaints is the role of the Information Commissioner. When making judgements about facts, administrative decision makers like the Commissioner make those judgements in terms of the civil standard of proof [and] the balance of probabilities…[A]n individual will be required to identify the respondent to the complaint. The operation of APP 8.1, in conjunction with [proposed] section 16C, means that it will not be necessary for an individual to identify the overseas recipient of the personal information as part of their complaint. The individual will only need to identify the relevant APP entity. The APP entity will be responsible (that is, accountable) for the acts and practices of the overseas recipient.[100]

International agreements relating to information-sharing

2.90 In relation to APP 8.2(e), the OAIC queried the effectiveness of the provision which, according to the EM, is intended to include all forms of information-sharing agreements made between Australia and international counterparts (such as treaties and exchanges of letters).[101] The OAIC submitted that, since an international agreement is not effective until it is incorporated into domestic law, international agreements cannot affect rights or obligations in Australian law. On this basis, the OAIC suggested:

> [S]pecific domestic legislative authority should be the basis for the exception in relation to the overseas disclosure of personal information under an international agreement.[102]

Departmental response

2.91 The Department noted that APP 8 reflects a new policy approach to the cross-border disclosure of personal information and rejected arguments that this approach will undermine privacy protection:

> The accountability approach in APP 8 will ensure effective cross-border protection for the personal information for individuals and is consistent with both [Organisation for Economic Co-operation and Development] and APEC privacy developments. APP 8 ensures that individuals whose information is disclosed to an overseas recipient continue to have an

99 Section 36 of the *Privacy Act 1988* (Privacy Act); proposed new subsection 13(1) of the Privacy Act (item 42 of Schedule 4 of the Bill).

100 Answer to question on notice, received 3 September 2012, p. 10.

101 EM, p. 85.

102 *Submission 47*, p. 20. Also see the Australian Privacy Foundation, which argued that APP 8.2(e) should be removed from the Bill on the grounds that it cannot be justified: see *Submission 49*, p. 19.

> Australian entity that is responsible for the protection of their personal information.[103]

2.92 APP 8.1 and proposed new section 16C do not contain any general exceptions: the only exceptions to the accountability regime are set out in APP 8.2. The Department stated:

> The exceptions in APP 8.2 have been carefully considered and the Government considers that they are justified. The Government considers that these exceptions provide appropriate and reasonable grounds for the transfer of accountability to an overseas recipient. In all other situations, the Australian entity should continue to remain accountable for the protection of personal information.[104]

Definitions

2.93 Items 4-45 of Schedule 1 of the Bill amend and repeal existing definitions in subsection 6(1) of the Privacy Act, as well as insert new definitions into the Privacy Act. Item 82 of Schedule 1 of the Bill also inserts new definitions relating specifically to the APPs. The proposed new definitions of 'enforcement body', 'enforcement related activity', and 'permitted general situation'/'permitted health situation' are discussed below.

'Enforcement body'

2.94 Items 16-19 of Schedule 1 of the Bill insert a number of agencies into the current definition of 'enforcement body' in subsection 6(1) of the Privacy Act.[105] The EM explains that these amendments will enable the body concerned to collect personal information (including 'sensitive information') related to the body's functions and activities, and to enable such information to be used or disclosed on its behalf for an 'enforcement related activity'.[106]

2.95 The addition of the 'Immigration Department'[107] (currently the Department of Immigration and Citizenship (DIAC))[108] as an 'enforcement related body' (item 17 of

---

103 Additional information, received 29 August 2012, p. 13.

104 Additional information, received 29 August 2012, p. 13.

105 The bodies to be included in the expanded definition of 'enforcement body' are: the CrimTrac Agency (item 16); the Immigration Department (item 17); the Office of the Director of Public Prosecutions, or a similar body established under a law of a state or territory (item 18); and the Corruption and Crime Commission of Western Australia (item 19).

106 EM, p. 57. The EM notes that the addition of the Office of the Director of Public Prosecutions and the Corruption and Crime Commission of Western Australia are for clarity and consistency only.

107 Item 26 of Schedule 1 of the Bill defines 'Immigration Department' to mean the Department administered by the Minister administering the *Migration Act 1958* (Cth).

108 EM, p. 57.

Schedule 1 of the Bill) particularly concerned the OAIC and the Australian Privacy Commissioner, Mr Timothy Pilgrim.

2.96 In its submission, the OAIC noted that item 17:

> …has the effect of bringing the Immigration Department within the enforcement related exceptions that appear throughout the APPs. For example, APP 3.4(d)(i) permits the Immigration Department to collect sensitive information about an individual without their consent, if it is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the Immigration Department.[109]

2.97 The OAIC pointed out that the 'Immigration Department' is not currently an 'enforcement body' under the Privacy Act, and the Exposure Draft of the Bill did not propose to make that inclusion. Further:

> The Immigration Department would appear to be of a different character to the other agencies included within the definition of an 'enforcement body', in the sense that its usual activities are not of an enforcement related nature. Accordingly, the OAIC believes that the Immigration Department's concerns are more appropriately addressed in enabling legislation, or alternatively under the Commissioner's power to make a [Public Interest Determination]. The OAIC recommends that the Immigration Department be removed from the definition of 'enforcement body'.[110]

Departmental response

2.98 The EM contains the following justification for the inclusion of the 'Immigration Department' as an 'enforcement body' under the Bill:

> In view of DIAC's enforcement related functions and activities, and the type of information it collects, uses and discloses, it is appropriate to include it in the definition of 'enforcement body'. However, given that it has a range of non-enforcement functions and activities, it will be limited in the collection of sensitive information to its 'enforcement related activities'.[111]

'Enforcement related activity'

2.99 Item 20 of Schedule 1 of the Bill inserts a new definition of 'enforcement related activity' into subsection 6(1) of the Privacy Act. The EM advises that the new definition will substantially capture the matters covered by NPP 2.1(h),[112] with the

---

109 *Submission 47*, p. 12.

110 *Submission 47*, p. 13. In contrast, the Law Institute of Victoria argued that exemptions for agencies should be set out in a schedule to the Privacy Act rather than in enabling legislation: see answer to question on notice, received 23 August 2012, pp 2-3.

111 EM, p. 57. The EM does not identify the types of sensitive information which could be collected by the Immigration Department in relation to its enforcement related activities.

112 NPP 2.1(h) creates an exception to the prohibition against organisations using or disclosing personal information for a secondary purpose by listing a number of activities conducted by or on behalf of law enforcement bodies in respect of which personal information may be used or disclosed: see EM, p. 58.

addition of paragraphs to cover the conduct of surveillance activities, intelligence gathering activities and other monitoring activities (proposed new paragraph (b) of the definition), as well as protective or custodial activities:

> These types of activities have been included to update and more accurately reflect the range of activities that law enforcement agencies currently undertake in performing their legitimate and lawful functions.[113]

2.100 Liberty Victoria expressed concern with proposed new paragraph (b) of the definition, arguing that it is too extensive and fails to balance the needs of enforcement agencies with the wider public interest of the community:

> There is neither a definition of 'surveillance activities' nor 'monitoring activities' found in the Bill and, as such, there is little to guide enforcement agencies and agencies to whom they are responsible as to what is legitimate and illegitimate use of private information. Further, enforcement agencies that conduct intelligence gathering activities are, in many respects, immune from external investigation as to the propriety of their activities. Liberty [Victoria] submits that in these circumstances there is a real and alarming potential for the improper use and disclosure of private information including biometric data.[114]

2.101 The Privacy Foundation argued similarly:

> It is not clear why [proposed new paragraph (b)] is considered necessary, and [it] has the potential to be very widely interpreted, and potentially misused to extend the effect of the exceptions which rely on the definition.[115]

'Permitted general situation' and 'permitted health situation'

2.102 Item 82 of Schedule 1 of the Bill inserts proposed new sections 16A and 16B into the Privacy Act. These provisions will allow an APP entity to collect, use or disclose personal information about an individual, or of a government-related identifier of an individual, in certain circumstances. Proposed new section 16A will set out exceptions described as 'permitted general situations', and proposed new section 16B will set out those exceptions described as 'permitted health situations'.

2.103 In accordance with Recommendation 1 of the F&PA committee's report, the APPs were restructured to reduce their length and to avoid repetition.[116] The Law Council contended, however, that locating proposed new sections 16A and 16B separately to the APPs may create confusion:

> For example, proposed section 16A which specifies 'permitted general situations' in which collection, use and disclosure of certain information by

113 EM, p. 58.

114 *Submission 13*, p. 2.

115 *Submission 49*, pp 8-9.

116 Attorney-General's Department, answer to question on notice, received 3 September 2012, p. 2.

> certain entities is allowed despite the APPs. As the APPs will not on their own set out all the circumstances in which a use or disclosure may occur, non-lawyers may find it difficult to identify the relevant rules. The [Law Council] suggests that notes be inserted in appropriate places in the Bill to draw the reader's attention to the existence and basic effect of those exceptions which are located in separate provisions rather than in the APPs.[117]

'Permitted general situation'

2.104 In relation to proposed new section 16A of the Privacy Act, the exceptions are set out in a table (proposed new subsection 16A(1)). For example, a 'permitted general situation' will exist in relation to personal information where an agency 'reasonably believes that the collection, use or disclosure is necessary for the entity's diplomatic or consular functions or activities'.[118]

2.105 The OAIC commented specifically on the inclusion of diplomatic or consular functions or activities as an exception to the APPs:

> The intended scope of the exception...and the specific information handling practices of [the Department of Foreign Affairs and Trade (DFAT)] that it is intended to address, are not clear. In particular, the term 'diplomatic and consular functions or activities' is not defined and, as such, could cover a broad range of circumstances that involve the collection, use or disclosure of personal information.[119]

2.106 The OAIC recommended removing the exception for diplomatic or consular functions or activities in proposed new subsection 16A of the Privacy Act:

> The OAIC acknowledges that there may be a public interest in exempting certain information handling activities undertaken by DFAT from the requirements of the APPs. However, the OAIC considers…that if these practices are not otherwise permitted by the Bill, they are more appropriately addressed in the agency's enabling legislation or, where no appropriate enabling legislation exists, via the Commissioner's power to make a [Public Interest Determination (PID)]. For example, since 1998 PID 7 and PID 7A have permitted DFAT to disclose the personal information of Australians overseas to their next of kin, in certain limited circumstances, where it would otherwise contravene the requirements of IPP 11.[120]

---

117 *Submission 14*, p. 8. For example, proposed new section 16A of the Privacy Act is used in APP 3.4 (Collection of sensitive information without the consent of the individual); APP 6.2 (Use or disclosure of personal information without the consent of the individual); and APP 8.2 (Disclosure of personal information to overseas recipients).

118 Item 6 in the table to proposed new subsection 16A(1) of the Privacy Act.

119 *Submission 47*, p. 11.

120 *Submission 47*, p. 12.

CHAPTER 3

Credit reporting definitions

3.1 Schedule 2 of the Bill reforms the regulation of credit reporting in an attempt to more accurately reflect the information flows within the credit reporting system and the general obligations set out in the Australian Privacy Principles.[1] A brief overview of the credit reporting system is provided in this chapter to provide context,[2] followed by a discussion of some of the proposed credit reporting definitions in Schedule 2 of the Bill and the related definition of 'Australian link' in Schedule 4 of the Bill.

Overview of the credit reporting system

3.2 New Part IIIA of the *Privacy Act 1988* (Privacy Act) sets out provisions in relation to the privacy of information related to credit reporting (credit reporting provisions).[3] The credit reporting provisions will apply to three main categories of participants in the credit reporting system: 'credit reporting bodies'; 'credit providers'; and 'affected information recipients'.[4] These terms are defined in the Bill and have specific meanings.[5]

3.3 The credit reporting system deals with categories of credit-related personal information. The Explanatory Memorandum (EM) states that it is necessary to use a number of specific terms to accurately describe the information flows within the credit reporting system:

> Because credit reporting bodies and credit providers may use personal information in the credit reporting system to derive and add new personal information to the system, it is important to accurately describe this process through the use of specific and defined terms. The key terms are: credit information; credit reporting information; credit eligibility information; and regulated information.[6]

---

1 Explanatory Memorandum (EM), p. 92.

2 The EM provides a more detailed explanation: see pp 93-98.

3 Item 72 of Schedule 2 of the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Bill).

4 Proposed Divisions 2-4 in new Part IIIA of Schedule 2 of the Bill.

5 Item 26 of Schedule 2 of the Bill provides the meaning of 'credit reporting body'; proposed new section 6G of the *Privacy Act 1988* (Privacy Act) defines the term 'credit provider' (item 69 of Schedule 2 of the Bill); and item 3 of Schedule 2 of the Bill sets out the definition of 'affected information recipient'.

6 EM, p. 93.

3.4 The definition of 'credit information' is discussed later in this chapter;[7] and 'credit reporting information' is defined as 'credit information' that has been disclosed to the 'credit reporting body' by the 'credit provider', as well as 'CRB derived information'.[8] 'Credit eligibility information' will mean 'credit reporting information' that was disclosed to the 'credit provider' by a 'credit reporting body' and 'CP derived information'.[9] 'Regulated information' will be 'credit eligibility information' or 'credit reporting information' that has been disclosed to 'affected information recipients'.[10]

3.5 The EM explains that there are two main features of the credit reporting system: first, the input side, where 'credit providers' put information into the system by disclosing the categories of personal information to 'credit reporting bodies'; and second, the output side, where 'credit reporting bodies' disclose certain personal information to 'credit providers', consistent with the permitted disclosures:[11]

> Generally, information only comes out of the system following requests from credit providers to credit reporting bodies for disclosure for specified purposes (or where disclosures are permitted to certain recipients for certain purposes by operation of the provisions, such as to an affected information recipient, or where disclosure is permitted by operation of an exception, such as where a disclosure is required or authorised by or under an Australian law or court or tribunal order).[12]

---

7 Proposed new section 6N of the Privacy Act; item 69 of Schedule 2 of the Bill. 'Credit information' is the basic unit of personal information within the credit reporting system. It is defined as comprising certain categories of personal information about an individual (other than sensitive information).

8 Item 28 of Schedule 2 of the Bill. Item 14 of Schedule 2 of the Bill defines the term 'CRB derived information' to mean personal information about an individual derived by a credit reporting body from credit information about the individual that is held by the credit reporting body and which has some bearing on an individual's credit worthiness, and will be used (or has been used, or could be used) to establish the individual's eligibility for consumer credit.

9 Item 17 of Schedule 2 of the Bill. Item 13 of Schedule 2 of the Bill defines the term 'CP derived information' to mean any personal information about an individual that is derived from credit reporting information that was disclosed to the credit provider by a credit reporting body under Division 2 and which has any bearing on an individual's credit worthiness, and will be used (or has been used, or could be used) to establish the individual's eligibility for consumer credit.

10 Item 55 of Schedule 2 of the Bill.

11 EM, p. 93.

12 EM, p. 94.

3.6 The use and disclosure of the relevant types of personal information are regulated by the credit reporting provisions, which provide different requirements for the participants based on whether they are taking part in the input side or the output side of the credit reporting system:

> This means, for example, that there can't be a single disclosure rule for credit providers, both because they have different roles in the system and because the personal information changes as it goes through the system. For this reason, there are provisions relating to the disclosure by credit providers to credit reporting bodies of credit information into the credit reporting system (and a related rule for credit reporting bodies dealing with collection of credit information). However, there are separate provisions relating to the disclosure by credit reporting bodies to credit providers, since the personal information disclosed will be credit reporting information...There is not one single category of personal information that can be regulated by a single rule that will apply in every case.[13]

Definitions

3.7 Schedule 2 of the Bill sets out amendments relating to general definitions in subsection 6(1) of the Privacy Act[14] and key definitions relating to credit reporting.[15] Many submitters commented on these proposed amendments, with commentary ranging from general to very specific issues.

General matters of interpretation

3.8 For some submitters, the number of definitions and their location within the Privacy Act was a concern. For example, the Australasian Retail Credit Association (ARCA) submitted that the Bill identifies 17 different classes of personal information, which leads to unnecessary complication and duplication.[16] The Australian Privacy Foundation similarly commented that the number of new, revised or defined credit reporting definitions:

> …hardly constitutes the 'simplification' desired by all parties and promised in the EM, and we submit that the scheme is now effectively too complex to be readily explicable, posing a serious risk of non-compliance and/or inability of consumers to effectively exercise their rights.[17]

---

13 EM, p. 96.

14 Items 2-65 of Schedule 2 of the Bill.

15 Proposed new Division 2 of Part II of the Privacy Act; item 69 of Schedule 2 of the Bill.

16 *Submission 27*, p. 12. For similar comments, also see Communications Alliance, answer to question on notice, received 23 August 2012, p. 1.

17 *Submission 49*, p. 26. Also see EM, p. 3.

3.9 The Law Council of Australia agreed that 'the use of multiple different named categories of credit-related information…may over-complicate the drafting'.[18] Its submission expressed further concern about:

> …certain structural elements of the Bill…One such concern is the structure whereby key concepts are defined in several places within the Bill, but distant from the Part IIIA context in which they are used. [19]

3.10 ARCA suggested as a solution the inclusion of a single definitions directory within the Bill.[20] However, the Office of the Australian Information Commissioner (OAIC) had an alternative recommendation for improving the interpretation of Schedule 2 of the Bill. Rather than restructure the proposed credit reporting definitions, the OAIC suggested including the credit reporting provisions as a schedule in the Privacy Act:

> The Explanatory Memorandum clarifies that the insertion of the APPs in a Schedule to the Privacy Act is intended to facilitate ease of reference to the APPs. The OAIC suggests that this consideration is equally relevant to the credit reporting provisions. Placing the credit reporting provisions in a Schedule to the Privacy Act will also ensure that provisions relevant only to specific industry sectors do not add complexity and length to the body of the Privacy Act.[21]

3.11 In May 2012, the Australian Government responded to the Senate Finance and Public Administration Legislation Committee's (F&PA committee) inquiry into the Exposure Draft of the Bill (F&PA inquiry). Consistent with the OAIC's suggestion to the current inquiry and the F&PA inquiry, the F&PA committee recommended that consideration should be given to locating the credit reporting provisions in a schedule to the Privacy Act.[22] The Australian Government, however, did not accept that recommendation:

> The Government considered the location of the credit reporting provisions and determined they are best located in the same place as the existing provisions.[23]

---

18 *Submission 14*, p. 11.

19 *Submission 14*, p. 11.

20 *Submission 27*, p. 12.

21 *Submission 47*, p. 21. Also see EM, p. 2.

22 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 28 (Recommendation 1).

23 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 3.

Departmental response

3.12 The Attorney-General's Department (Department) informed the committee that it has implemented ALRC Recommendation 5-2, which supported redrafting the Privacy Act to achieve greater logical consistency, simplicity and clarity.[24] The Department advised further that it considers that the drafting style adopted in the Bill reflects current best drafting practice and effectively balances competing interests.[25]

3.13 Specifically in relation to the credit reporting provisions, the Department provided the following comprehensive explanation for the way in which the provisions are presented in the Bill:

> Consistent with modern drafting practices and the approach adopted throughout the Bill, each division in Part IIIA that deals with substantive rights and obligations commences with a guide to assist the reader [to] understand the content of the Division. In addition, clause 19 sets out a guide to Part IIIA as a whole. Guides were not inserted for Division 6 (which contains certain offences) or Division 7 (which deals with certain court orders) as these divisions are short and self-explanatory.
>
> In relation to the structure of the Bill, these privacy law reforms proceed by amending the existing Act, rather than by replacing the Act with an entirely new Act. This means that the structure of the final consolidated Act will remain consistent with the existing structure of the Act. Credit reporting definitions will be located in Part II – Interpretation, which currently contains all definitions and other provisions relevant to interpreting the Act.
>
> At present the credit reporting related provisions are in a number of different places in Part II of the Act. The Bill reorganises the definitions in Part II into a logical sequence and groups similar specific definitions together. Part II will be divided into two divisions – Division 1 will contain all the general definitions for the Act, while Division 2 will contain key definitions relating to credit reporting. Division 1 will include all the credit reporting definitions in subsection 6(1). Where terms require a more comprehensive definition, the reference in subsection 6(1) will point to the specific definition in Division 2. In this way, Division 1 will be the starting point for identifying and locating all defined terms in the amended Act. The Department considers that this approach to structuring the credit reporting provisions is consistent with the existing structure of the Act and, once amended, will be logical, straightforward and clear.[26]

---

24 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, p. 27.

25 Answer to question on notice, received 3 September 2012, p. 13.

26 Answer to question on notice, received 3 September 2012, pp 13-14.

'Australian link'

3.14 Items 2 to 65 in Schedule 2 of the Bill amend general definitions in subsection 6(1) of the Privacy Act. The general definition which most concerned submitters and witnesses is the term 'Australian link' in section 5B of the Privacy Act.

3.15 The EM states:

> The credit reporting system is restricted to information about consumer credit in Australia and access to the credit reporting system is only available to credit providers in Australia. The credit reporting system will not contain foreign credit information or information from foreign credit providers (even if they have provided credit to an individual who is in Australia), nor will information from the credit reporting system be available to foreign credit reporting bodies or foreign credit providers.[27]

3.16 To effect this policy proposal, the Australian Government considered a number of general provisions stating these limitations but:

> [I]t was considered that a simpler, clearer and more effective approach was to ensure appropriate limitations were in place in relation to each relevant provision dealing with the collection, use and disclosure of information by credit reporting bodies and credit providers in Part IIIA.[28]

General comment regarding the definition

3.17 Items 4 to 7 of Schedule 4 of the Bill will amend the definition of 'Australian link' in subsections 5B(2) and 5B(3) of the Privacy Act. The new definition will outline the circumstances in which an organisation or small business operator will have an 'Australian link'. For example, under proposed new paragraph 5B(3)(c) an 'Australian link' will exist where 'personal information was collected or held by the organisation or operator in Australia or an external Territory', and the other requirements of the section are satisfied.[29]

3.18 The EM states:

> The collection of personal information 'in Australia' under [proposed] paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.
>
> For example, a collection is taken to have occurred 'in Australia' where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website

---

27 EM, p. 91.

28 EM, p. 91. The Office of the Australian Information Commissioner submitted that the government's objective could be more effectively achieved with the use of specific exclusionary provisions: see *Submission 47*, pp 22-23.

29 Items 6-7 of Schedule 4 of the Bill.

> is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. It is intended that…entities…who have an online presence (but no physical presence in Australia) and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory'.[30]

3.19 The OAIC questioned whether the government's objective will be achieved with the use of the 'Australian link' term, contending that the intention stated in the EM is not reflected in the Bill. Its submission argued that the phrase 'in Australia' is not clear, particularly in the online context, and should be made explicit, for example, by amending 'in Australia' to read 'from Australia'.[31] At the first public hearing, the Australian Privacy Commissioner, Mr Timothy Pilgrim, specifically stated:

> [T]he use of the terminology 'in Australia' in the credit provisions may leave open to interpretation whether or not foreign credit reporting entities can get access to the information.[32]

3.20 For many other submitters, it was not the definition of the term 'Australian link', but the manner in which the term is to be applied throughout the credit reporting provisions, that raises concerns.

Extra-territorial operation

3.21 Several submitters and witnesses questioned the use of the term 'Australian link' in relation to proposed new paragraph 21G(3)(b) of the Privacy Act.[33] This provision will prevent a 'credit provider' who holds 'credit eligibility information' about an individual from using or disclosing that information to a related body corporate which does not have an 'Australian link'.

3.22 Industry submitters and witnesses argued that this use of the 'Australian link' requirement is excessive and inconsistent, and will significantly affect business operations.[34] In evidence, for example, Mrs Sue Jeffrey from ANZ Banking Group Limited (ANZ) argued:

> [T]he Australian link requirement will have a major effect on the way ANZ structures its businesses. For example, ANZ from time to time use[s] credit assessment teams in New Zealand to assist with processing home loan applications during periods of high volume. We would like to retain this ability to move work across our geographies in order to best meet the needs

30 EM, p. 218.

31 *Submission 47*, p. 17.

32 *Committee Hansard*, 10 August 2012, p. 12.

33 Item 72 of Schedule 2 of the Bill.

34 See, for example, Mr Steven Münchenberg, Australian Bankers' Association, *Committee Hansard*, 10 August 2012, p. 15; Mr John Stanton, Communications Alliance, *Committee Hansard*, 10 August 2012, p. 16.

> of our customers. [The Bill] would represent a much more significant impact than we expect was intended. It would be a backward step in ANZ's ability to structure its operations in a way that supports our regional footprint and delivers our customers efficient, high quality service. At the same time it would offer no additional privacy protection to our customers.[35]

3.23 The Law Council of Australia noted:

> [S]ome authorised deposit taking institutions have established outsourcing operations with entities based in foreign countries as a means of providing financial services more economically and contributing to lower overall prices…The offshore entities may be wholly-owned but foreign incorporated subsidiaries, or may be unrelated bodies subject to strict service agreements which require information to be used and dealt with solely for the purposes of the principal with high levels of security.[36]

Contrast with approach in APP 8

3.24 The Australian Bankers' Association (ABA) contrasted proposed new section 21G, which contains the general prohibition against the use or disclosure of 'credit eligibility information' by a 'credit provider', with cross-border disclosures of personal information (other than 'credit eligibility information') to overseas recipients under proposed Australian Privacy Principle 8 (APP 8):

> APP 8 together with proposed section 16C means a bank will remain liable if the overseas recipient of the personal information engages in conduct that would be a breach of an APP (other than APP 1) as if the conduct had occurred in Australia unless certain limited exceptions in APP 8.2 apply.[37]

3.25 The ABA submitted further:

> [T]here seems to be no logical reason why it is necessary for two different regimes to apply according to the type of personal information involved – the one, under the credit reporting provisions that imposes a complete prohibition on the disclosure of credit eligibility information to an overseas recipient where the recipient has no Australian link and the other, where the cross border disclosure of personal information other than credit eligibility information is subject to an accountability rule (section 16C) or specific exceptions.[38]

---

35 *Committee Hansard*, 10 August 2012, p. 15.

36 *Submission 14*, p. 14. Also see, for example, ANZ Banking Group Limited, *Submission 29*, p. 4; Australian Industry Group, *Submission 16*, p. 3.

37 *Submission 24*, p. 5. Also see item 104 of Schedule 1 of the Bill.

38 *Submission 24*, p. 6. The Australian Bankers' Association also noted that the existence of two different regulatory regimes will present operational difficulties for financial services businesses. For similar comments, see: Australasian Retail Credit Association, *Submission 27*, p. 6; GE Capital, *Submission 43*, p. 3.

3.26 The Australian Finance Conference, ANZ and Optus made similar comments, noting that the disclosure of equally sensitive personal information to overseas recipients is permitted under APP 8. For example, ANZ stated:

> The Bill allows the cross-border disclosure of other forms of sensitive information, such as health information and the customer's credit card transactions, provided the disclosing organisation complies with APP 8...It is not clear why the disclosure of ['credit eligibility information'] for legitimate business purposes should be treated more restrictively than information that is likely to be as sensitive.[39]

3.27 Several submitters recommended that the Bill should allow for the disclosure of 'credit eligibility information' (CEI) to overseas recipients under APP 8.[40] As ANZ argued:

> [T]he Australia link requirement [should] be removed for disclosure of CEI for legitimate business purposes to an offshore entity that is an agent or related body corporate of the disclosing entity. ANZ also recommends that APP 8 [should apply] to offshore disclosure of credit information in the same way it applies to other forms of personal information. These recommendations are predicated on the disclosing entity remaining responsible in the event of a privacy breach.[41]

Departmental response

3.28 In evidence, a representative from the Department confirmed that the Bill introduces for the first time a specific rule to deal with the cross-border disclosure of credit reporting information.[42] Departmental officers recognised that the implementation of this rule – using the 'Australian link' requirement – is problematic for some stakeholders due to the way in which they have structured their business operations:

> We are certainly not looking to get into a situation where we are trying to break business models that banks have established, but we are looking to reach a more targeted policy outcome.[43]

---

39 *Submission 29*, p. 4. Also see Optus, *Submission 31*, p. 8; Australian Finance Conference, *Submission 36*, p. 11.

40 See Australian Bankers' Association, *Submission 24*, p. 7; Australasian Retail Credit Association, *Submission 27*, p. 6; GE Capital, *Submission 43*, p. 3.

41 *Submission 29*, p. 5. Also see Law Council of Australia, *Submission 14*, which argued that the 'artificial' 'Australian link' requirement should not apply where a credit provider is an authorised deposit-taking institution under the *Banking Act 1959* (Cth) and where the use of an offshore provider is consistent with standards set by the Australian Prudential Regulation Authority (APRA) and is subject to APRA's supervision: p. 14.

42 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 5.

43 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 5. Also see Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 2.

3.29 The officers also noted APP 8, which deals with the cross border disclosure of personal information (excluding 'credit eligibility information') and which has a related accountability mechanism in proposed new section 16C of the Privacy Act (item 82 of Schedule 1 of the Bill). They explained that it would not be appropriate to extend this regime to the credit reporting provisions:

> The structure of the credit reporting provisions is to prohibit all collection, use and disclosure of personal information in the credit reporting system and then provide targeted exceptions for permitted acts and practices…[T]he Department considers that simply applying APP 8 without any modification may undermine the policy of not disclosing Australian credit information to foreign credit providers. The Department's preferred approach is to identify options to provide specifically for a targeted disclosure (and associated use) to deal with off-shore processing. Such a targeted provision could then impose obligations based on APP 8.1 and proposed section 16C of the Privacy Amendment Bill to ensure that the Australian credit provider remains accountable for the personal information in the hands of the overseas processor recipient. Initial discussions with credit provider stakeholders indicate that this approach may be acceptable to them. We will continue to work with stakeholders to refine an approach that can be put to the Attorney-General for consideration.[44]

'Credit provider'

3.30 Submitters and witnesses were also concerned with certain key definitions relating to credit reporting in proposed new Division 2 of Part II of the Privacy Act,[45] including the definitions of: 'credit provider'; 'credit information'; 'default information'; 'serious credit infringement'; 'new arrangement information'; and 'repayment history information'.

3.31 Proposed new section 6G (item 69 of Schedule 2) inserts a definition of the key term 'credit provider' into the Privacy Act. The definition will include a 'bank' and will allow for certain inclusions and exclusions, such as a class of organisations or small business operators prescribed by the regulations (proposed new subsection 6G(6)).

---

44 Additional information, received 29 August 2012, p. 6. Also see Mr Colin Minihan, Attorney-General's Department, *Committee Hansard,* 21 August 2012, p. 2; Mr Richard Glenn, Attorney-General's Department, *Committee Hansard,* 21 August 2012, p. 3.

45 Item 69 of Schedule 2 of the Bill.

3.32 In relation to 'credit provider', submitters directed their comments toward the breadth or, conversely, the lack of breadth in the new definition.[46] For example, Min-it Software argued that proposed new paragraph 6G(2)(b) of the Privacy Act[47] widens the current definition of 'credit provider' 'solely for the benefit of the credit reporting businesses':

> Australian Credit Licence ("ACL") holders already have to hold and retain far more personal information than is really necessary due to [the National Consumer Credit Protection] Act, the [credit reporting] Code and [the Australian Securities and Investments Commission's] requirements but rather than further limiting who has access to personal information, this Bill will allow additional credit providers to seek, hold and collect personal information they currently cannot access. Consequently, if many others have access to an individual's personal information through their work, an individual's right to privacy has been considerably and directly diminished by this legislation.[48]

3.33 On the other hand, the Communications Alliance queried whether telecommunications providers are captured by the definition and noted that proposed new subsection 6G(6) of the Privacy Act could result in its members being excluded from the new definition of 'credit provider'.[49]

3.34 However, the Communications Alliance stated that one of its biggest concerns with the Bill is that it does not allow for the existence of different kinds of 'credit provider', the different sectors and industries involved, and the way in which each of these stakeholders uses 'credit information':

> We would suggest that the bill be reviewed with the objective of determining whether each of the credit provider rules is relevant across all industries and, if not, perhaps removing them from the bill and allowing that to be dealt with in the credit reporting code.[50]

---

46 For example, Abacus-Australian Mutuals queried whether the definition of 'credit provider' sufficiently identifies all institutions authorised to operate a banking business under the *Banking Act 1959*: see *Submission 25*, p. 6; GE Capital questioned the inclusion of retail stores in the definition of 'credit provider': see *Submission 43*, p. 2; and Finance Industry Delegation considered that the definition of 'credit provider' is too broad and should align with that contained in the *National Credit Consumer Protection Act 2009* (Cth): see *Submission 56*, pp 4-5.

47 Proposed new paragraph 6G(2)(b) of the Privacy Act will allow an organisation or small business operator who supplies credit for more than seven days in connection with the sale of goods, or the supply of services, to be treated as a 'credit provider' in relation to that credit.

48 *Submission 48*, pp 6-7.

49 *Submission 30*, p. 6.

50 Mr John Stanton, Communications Alliance, *Committee Hansard*, 10 August 2012, p. 16. Also see Telstra, which made similar comments regarding the different regimes under which credit providers operate and how these regimes should be accommodated within the proposed legislative framework: *Submission 52*, p. 3.

'Credit information'

3.35 Proposed new section 6N (item 69 of Schedule 2) inserts a definition of the key term 'credit information' into the Privacy Act. This new definition comprises certain categories of personal information about an individual (other than sensitive information). Some of these categories will be further defined in subsection 6(1) of the Privacy Act, and some categories will be further defined in other proposed new sections contained in item 69 of Schedule 2 (Key definitions relating to credit reporting).

3.36 Submitters and witnesses commented on a variety of proposed definitions for categories of personal information comprising 'credit information'.[51] For example, Veda contended that the definition of 'identification information' (item 34 of Schedule 2) will affect the accuracy of approximately 2.4 million credit files and the ability of 'credit reporting bodies' to accurately match a credit inquiry to a file.[52] That new definition refers to an individual's current or last known address, and two previous addresses (if any).

3.37 At the first public hearing, a representative from Veda informed the committee:

> Veda is calling for credit-reporting bureaus to be able to hold the greater of current address plus two previous addresses or current address plus all previous addresses over the past five years. The reason why this is important is that there is a high-risk segment, generally younger people, who move address very frequently. Under the proposed legislation, we would lose all of the information that attaches to them once they have moved address more than twice, so we would very much like that to be remedied in the bill.[53]

3.38 The Department did not agree that 'credit reporting bodies' would 'lose all information about an individual if the individual moves more than twice in [a] five year period':

> [T]he proposed definition of 'identification information' includes a range of other types of personal information…The Department considers that the various types of personal information included in the definition of 'identification information', in conjunction with the permitted address information, should be sufficient to identify individuals.[54]

---

51 For example, Liberty Victoria commented on the new definition of 'court proceedings information': see *Submission 13*, pp 1-2; item 12 of Schedule 2 of the Bill.

52 *Submission 41*, pp 1-2.

53 Dr David Grafton, Veda, *Committee Hansard*, 10 August 2012, p. 23.

54 Additional information, received 29 August 2012, pp 8-9.

'Default information'

3.39 Proposed new subsection 6Q(1) (item 64 of Schedule 2) inserts a definition of the key term 'default information' into the Privacy Act in relation to consumer credit defaults. 'Default information' about an individual is information about an overdue payment (including one which is wholly or partially comprised of interest) in relation to consumer credit provided by a 'credit provider' to the individual if:

- the payment is at least 60 days overdue;
- the 'credit provider' has given the individual written notice informing the individual of the overdue payment and requesting that the individual pay the overdue amount;
- the 'credit provider' is not prevented by a statute of limitations from recovering the overdue amount; and
- the overdue amount is equal to or more than:
    - $100; or
    - such higher amount as is prescribed by the regulations.

3.40 Submitters raised a number of issues in relation to proposed new subsection 6Q(1) of the Privacy Act. For example, submitters expressed concerns regarding the interaction between the notification and listing processes, the threshold amount, when a default can be listed and for how long, and the interaction between the hardship provisions in the *National Consumer Credit Protection Act 2009* (National Consumer Credit Protection Act) and the default provisions in privacy legislation.

Notification and listing processes

3.41 The Consumer Credit Legal Centre (NSW) (CCLCNSW) submitted that the proposed provision is problematic for consumers 'as it allows credit providers to subvert the process to disadvantage consumers'. CCLCNSW's submission argued that a 'credit provider' could list a default immediately after issuing written notice to an individual:

> This is procedurally unfair as it is the notice that is important in notifying the consumer that there actually is a default! It is more than possible to be unaware of the default simply because there was a bank error in direct debits for example.[55]

3.42 CCLCNSW recommended that proposed new paragraph 6Q(1)(b) should be amended to require 30 days to have elapsed from the date of the written notice before

55 *Submission 51*, p. 14. For similar comments, also see Australian Communications Consumer Action Network, *Submission 50*, p. 7; and Hunter Community Legal Centre, *Submission 33*, p. 7 (in relation to 'serious credit infringements').

listing can occur.[56] In the same vein, the Australian Communications Consumer Action Network (ACCAN) called for a mechanism whereby consumers can challenge listings when they have had no opportunity to be notified about an imminent listing:

> ACCAN recommends that there be a specific notification requirement related to the intention to credit list and that this requirement be such that all reasonable attempts to contact the customer with a specific warning should be a prerequisite to credit listing.[57]

Threshold amount

3.43 In relation to the threshold amount stipulated in proposed new subparagraph 6Q(1)(d)(i), the Energy & Water Ombudsman NSW (EWON) supported prescribing a minimum amount but suggested that a more realistic definition of the overdue amount would be in the order of $300: 'This would exclude small utility bills from the adverse consequences of credit listing'.[58] ACCAN and CCLCNSW concurred,[59] whereas the Hunter Community Legal Centre submitted that the minimum amount should be $500 (excluding interest).[60] Mr Pilgrim agreed that 'there is some merit in looking at that [$300] level'.[61]

Default listings

3.44 Both EWON and the Financial Ombudsman Service (FOS) noted that the Bill does not specify when 'default information' can be listed.[62] EWON advised that, in its experience:

> [S]ome customers are credit default listed but there is a delay in the listing, sometimes up to several years after the subject debt arose. This means that the negative impact on a customer's credit report will continue well beyond the usual five year period of a credit default listing. It may also run over the standard period of time a provider has to take legal action to recover a debt. It seems unreasonable and unfair for the effects of a debt to be prolonged in this way.[63]

---

56 *Submission 51*, p. 14.

57 *Submission 50*, p. 7. Also see Hunter Community Legal Centre, which recommended that credit providers should be required to undertake increased contact with consumers when a default occurs and when listing occurs: *Submission 33*, p. 5; and the Financial Ombudsman Service, which called for proximate notification of an intention to list: *Submission 12*, pp 2-3.

58 *Submission 38*, p. 3.

59 *Submission 50*, p. 8 and *Submission 51*, p. 14, respectively.

60 *Submission 33*, p. 5.

61 *Committee Hansard*, 21 August 2012, p. 8.

62 *Submission 38*, p. 4 and *Submission 12*, p. 5, respectively.

63 *Submission 38*, p. 4.

3.45 EWON submitted that it would be useful if the Bill were to provide clarification on this issue,[64] whereas the FOS submitted:

> [M]andating in legislation a 12 month 'limitation period' is not sufficiently flexible to deal with the broad range of financial circumstances that give rise to default listings…A likely response from many Financial Services Providers will be to no longer act with discretion and default list all overdue customers within 12 months of the account falling more than 60 days overdue.[65]

3.46 In its inquiry, the F&PA committee received similar evidence regarding the timeframe for the disclosure of 'default information'. That committee recommended that greater clarity should be provided by either the OAIC or in the credit reporting code,[66] a recommendation which was accepted by the Australian Government.[67]

3.47 EWON also noted that a listing is for a period of five years (item 4 in the table to proposed new section 20W of the Privacy Act, contained in item 72 of Schedule 2 of the Bill) regardless of whether the default amount is $300 or $30,000. EWON suggested:

> [A]nother option could be a 'sliding scale' where the credit default listing is for a period relative to the amount of the debt, e.g. $1000 or less = 1 year listing; $1001 to $5000 = 2 years listing; $5001 to $10,000 = 3 years listing etc.[68]

3.48 ACCAN agreed that listings should be proportionate to the default amount and, in any event, two years for telecommunications products.[69] CCLCNSW endorsed this view with respect to listings related to credit which is not regulated by the National Consumer Credit Protection Act:

> [I]t is unreasonable and excessive to hold default information on utilities and other debts (that are not credit as defined under the National Consumer

64 *Submission 38*, p. 4. Some submissions noted that the Telecommunications Industry Ombudsman has adopted the approach that an overdue account should not be listed more than 12 months after the account due date: see, for example, Australian Communications Consumer Action Network, *Submission 50*, p. 8.

65 *Submission 12*, pp 5-6.

66 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 131 (Recommendation 20).

67 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 9.

68 *Submission 38*, p. 3.

69 *Submission 50*, p. 8.

> Credit Protection Act) for [five years]…[T]he retention period for default information on a consumer's credit report for utilities should be two years.[70]

National Consumer Credit Protection Act 2009

3.49 Some submitters drew attention to the interaction between the hardship provisions in the National Consumer Credit Protection Act[71] and the default provisions in the Bill.[72] The FOS, for example, advised that a common and increasing basis for complaints is that an individual is listed while negotiating a hardship arrangement. The FOS suggested that the Bill address the interrelationship between the two regimes:[73]

> [E]ither the [Bill] or the Code of Conduct should set some parameters as to a Financial Services Provider's obligation to properly consider any application by a borrower for financial difficulty assistance before default listing that borrower.[74]

3.50 ARCA similarly suggested alignment of the two legislative regimes by using the proposed credit reporting code (to be created under Schedule 3 of the Bill) to achieve that objective:

> [This] will allow better alignment between the Privacy Act and the National Consumer Credit Protection Act arrangements.[75]

'Serious credit infringement'

3.51 Item 63 of Schedule 2 of the Bill repeals and replaces the definition of 'serious credit infringement' in current subsection 6(1) of the Privacy Act. 'Serious credit infringement' will mean:

> (a) an act done by an individual that involves fraudulently obtaining consumer credit, or attempting fraudulently to obtain consumer credit; or

---

70 *Submission 51*, p. 19. Also see proposed new section 20W of the Privacy Act (item 72 of Schedule 2 of the Bill).

71 Division 3 of Part IV of the National Credit Code in Schedule 1 of the *National Consumer Credit Protection Act 2009*. Section 72 of that Act provides that, under certain circumstances, a debtor who is reasonably unable to meet his or her obligations under a credit contract may apply to a credit provider for a variation of the terms of the contract.

72 For example, Financial Ombudsman Service, *Submission 12*, pp 3-4; Consumer Action Law Centre, *Submission 5*, p. 7; Consumer Credit Legal Centre (NSW), *Submission 51*, p. 9.

73 *Submission 12*, pp 3-4. Also see Consumer Credit Legal Centre (NSW), which argued that credit providers should not be able to default list a consumer who has entered into a hardship arrangement: *Submission 51*, p. 9.

74 Answer to question on notice, received 23 August 2012, p. 3.

75 *Submission 27*, p. 17. Also see Consumer Credit Legal Centre (NSW), answer to question on notice, received 23 August 2012, p. 3.

> (b) an act done by an individual that involves fraudulently evading the individual's obligations in relation to consumer credit, or attempting fraudulently to evade those obligations; or
>
> (c) an act done by an individual if:
>
> > (i) a reasonable person would consider that the act indicates an intention, on the part of the individual, to no longer comply with the individual's obligations in relation to consumer credit provided by a credit provider; and
> >
> > (ii) the provider has, after taking such steps as are reasonable in the circumstances, been unable to contact the individual about the act; and
> >
> > (iii) at least 6 months have passed since the provider last had contact with the individual.

3.52 The CCLCNSW and the Consumer Action Law Centre (CALC) submitted that the proposed new definition of 'serious credit infringement' (SCI) is one of the most critical consumer issues in the Bill. The CALC argued:

> It is difficult to understate the significance of a credit provider listing an SCI on a consumer's credit report. An SCI is the most serious type of listing that can be made apart from bankruptcy, and yet it is the only listing that can be made based purely on the opinion of a credit provider at a particular point in time.
>
> Once made, an SCI will ordinarily remain on a credit report for seven years. They can be very difficult to remove earlier – even if the consumer can demonstrate that, had the credit provider known all the circumstances, they would not have made the listing. Further, it is often the case that SCIs are listed merely because of an error, misunderstanding or breakdown in communications.[76]

Six-month waiting period

3.53 The CALC expressed concerns in relation to the six-month waiting period in proposed subparagraph (c)(iii), which it submitted does not require a 'credit provider' to attempt to contact a customer or review the appropriateness of the listing after six months.[77] The FOS, which supported the proposed provision, submitted:

> [I]t is appropriate that the…Bill include a requirement that the Financial Services Provider must have taken reasonable steps to contact an individual and that at least 6 months should have passed without contact prior to entering a serious credit infringement listing.[78]

---

76 *Submission 5*, p. 2. Also see Consumer Credit Legal Centre (NSW), *Submission 51*, p. 3. The Hunter Community Legal Centre made similar comments regarding the circumstances in which a 'serious credit infringement' can be listed: see *Submission 33*, p. 7.

77 *Submission 5*, p. 4.

78 *Submission 12*, p. 6.

Evidence to the F&PA committee's inquiry and government response

3.54 The CALC referred to the F&PA inquiry where Veda Advantage (now Veda) and a number of consumer advocates suggested that the definition of 'serious credit infringement' should be replaced with two new definitions: 'un-contactable default' and 'never paid' flag.[79] In its submission to the current inquiry, the CALC supported this proposal as more effective and proportionate:

> [I]t requires a 'never paid' flag to be automatically removed after six months (although a default would remain) and for 'un-contactable defaults' to be removed if contact is re-established at any point with the consumer.[80]

3.55 In its 2008 report, the Australian Law Reform Commission did not consider that 'serious credit infringements' should necessarily be limited to conduct that is fraudulent:

> Credit providers have a legitimate interest in sharing information about the conduct of individuals that falls short of fraud – for example, where an individual deliberately avoids contact with a credit provider in order to evade his or her financial responsibilities.[81]

3.56 Further, the Department of the Prime Minister and Cabinet (which then had portfolio responsibility for privacy matters) noted in its evidence to the F&PA inquiry that the proposal by Veda and consumer advocates:

> …appears to remove any element of fraudulent activity from consideration, apparently reclassifying serious credit infringements into a default that occurs when a person cannot be contacted.[82]

3.57 The F&PA committee accepted this evidence and noted its concern that the stakeholder proposal 'does not reflect the serious nature of intentional credit fraud as is provided for in the credit reporting system'.[83] That committee recommended:

---

79 An 'un-contactable default' would relate to situations in which a default has been listed, and the debtor has not responded and cannot be contacted throughout the default period. A 'never paid' flag would be a flag relating to telecommunications or utilities debts where, after 60 days, no payment is made on the account and the credit provider has reasonable grounds to believe that the consumer never had any intention to make a payment on the account: Senate Finance and Public Administration Legislation Committee, Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting, Veda Advantage, additional information, received 9 August 2011, p. 1.

80 *Submission 5*, p. 4.

81 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Volume 3, p. 78.

82 Senate Finance and Public Administration Legislation Committee, Inquiry into Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting, Department of the Prime Minister and Cabinet, additional information, received 2 September 2011, p. 3.

83 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 60.

> …that consideration be given to a change of approach in dealing with serious credit infringements to allow for those listings, not relating to intentional fraud, to be dealt with in a different manner.[84]

3.58 The Australian Government accepted this recommendation[85] and in response has inserted proposed subparagraph (c)(iii) into the new definition of 'serious credit infringement' in the current Bill.[86] According to the EM to the Bill, this is intended to provide 'a practical timeframe in which the individual may be able to pay the debt before a serious credit infringement is listed'.[87] In addition, the Department noted that the credit reporting code will:

> …provide further requirements and guidance in relation to the reasonable steps that a credit provider must take to contact an individual. This may include requirements relating to the number of attempts to contact the individual and other related matters.[88]

'New arrangement information'

3.59 Proposed new section 6S (item 69 of Schedule 2 of the Bill) inserts a definition of the term 'new arrangement information' into the Privacy Act. While similar to a hardship arrangement under the National Consumer Credit Protection Act, 'new arrangement information' is distinguishable by the point in time at which a 'credit provider' has disclosed the existence of 'default information' or a 'serious credit infringement':

> Where an individual is overdue in making payments in relation to consumer credit a credit provider may choose to enter into a new arrangement with the individual. Such a new arrangement only satisfies the definition of 'new arrangement information' if the credit provider has previously disclosed 'default information' or a 'serious credit infringement' in relation to the individual's overdue payments [that is, a listing has occurred]…In some circumstances prior to a default, the credit provider and the individual may agree on a hardship arrangement, as provided for in the [National Consumer Credit Protection] Act. Hardship arrangements that satisfy the requirements of the [National Consumer Credit Protection] Act are not included within the meaning of 'new arrangement information'.[89]

---

84 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 60 (Recommendation 8).

85 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 5.

86 Attorney-General's Department, answer to question on notice, received 3 September 2012, p. 16.

87 EM, p. 116.

88 Answer to question on notice, received 3 September 2012, p. 16.

89 EM, p. 127.

3.60 Two submitters – ARCA and ANZ – commented on the Bill addressing only situations involving post-default hardship. Both noted that pre-default hardship arrangements would not come to the attention of other participants in the credit reporting system, potentially leading to consumer detriment due to the reporting of adverse repayment history. As ANZ explained:

> Where a temporary arrangement is in place, and even though an individual is meeting the terms of that arrangement, credit providers will be required to report that the individual did not make their required monthly payment. The consequence is that an individual who is complying with a temporary arrangement will be treated in the same way as an individual who has simply failed to make required payments.[90]

3.61 ANZ argued that 'credit providers' should be able to accurately report the status of a customer experiencing temporary hardship but who is making agreed payments:

> [T]he Bill should provide a mechanism to indicate that an individual is subject to a hardship arrangement, such as a temporary hardship flag. The flag would only be visible when the individual was in a hardship arrangement and would be removed once the hardship arrangement ended. Such an approach would reduce the chance of a consumer in hardship being inappropriately provided additional credit but would not adversely impact the ability of the consumer to obtain credit in the future.[91]

3.62 Mr David Niven from the Financial Ombudsman Service told the committee that the difficulty is that 'the ground rules as to how [financial hardship] ought [to] be treated by a credit provider acting in good practice are unclear':

> [A consumer] will be making a payment arrangement but [they] will nonetheless be behind on [their] contractual repayments. There will then be an issue as to whether or not that is a variation: is that a binding variation so that I am no longer a consumer in default, or is it, as the upmarket lawyers call it, simply an indulgence so that they are prepared to accept that without prejudice to their rights and I could still be listed?[92]

3.63 Ms Katherine Lane from CCLCNSW thought it better that the Bill remain silent on these issues:

> [I]t is essential that consumers are encouraged to request financial hardship when needed. If there is a negative consequence of doing that, that would be very unfortunate. I support the bill being silent on this issue. I think it is something that could be worked out perhaps in the [regulations] or the code.[93]

---

90 *Submission 29*, p. 5. Also see Australasian Retail Credit Association, *Submission 27*, p. 17.

91 *Submission 29*, p. 6.

92 *Committee Hansard*, 10 August 2012, p. 31.

93 *Committee Hansard*, 10 August 2012, p. 31.

Departmental response

3.64 The Department recognised that the credit reporting industry has called for a 'hardship flag' to be included in the 'credit information' of an individual who has been provided with a hardship variation under section 72 of the National Consumer Credit Protection Act. However, this argument has been rejected by the Australian Government:

> Hardship variations cannot be listed as part of an individual's credit reporting information. The Government is concerned that permitting the listing of hardship variations may act as a deterrent to individuals seeking hardship variations in appropriate circumstances (including following a natural disaster) and this would be contrary to the intention of providing the right to request a hardship variation.[94]

'Repayment history information'

3.65 The introduction of more comprehensive, or positive, credit reporting to provide additional information about an individual's ongoing credit arrangements is one of the five major reforms contained in Schedule 2 of the Bill.[95] This reform will introduce five new data sets into the credit reporting system, one of which will be 'repayment history information'.

3.66 Proposed new subsection 6V(1) (item 69 of Schedule 2) inserts a definition of the term 'repayment history information' into the Privacy Act. 'Repayment history information', in relation to consumer credit given to an individual by a 'credit provider', will mean:

- whether or not the individual has met an obligation to make a monthly payment that is due and payable;
- the day on which the monthly payment is due and payable; and
- if the individual makes the monthly payment after the day on which the payment is due and payable – the day on which the individual makes that payment.

3.67 Most submitters and witnesses commented on the application of the term 'repayment history information' within proposed new Part IIIA of the Privacy Act (item 72 of Schedule 2).[96] However, ARCA argued that the new definition of

---

94 Answer to question on notice, received 3 September 2012, p. 15. The Australian Government has not accepted the listing of hardship variations as a necessary component of the credit reporting system: see p. 17.

95 EM, p. 92.

96 For example, see: Insurance Council of Australia, *Submission 23*, p. 2; Diners Club International, *Submission 28*, pp 1-2; Min-it Software, *Submission 48*, p. 11; Mr John Stanton, Communications Alliance, *Committee Hansard*, 10 August 2012, p. 16; Ms Katherine Lane, Consumer Credit Legal Centre (NSW), *Committee Hansard*, 10 August 2012, p. 30.

'repayment history information' is inconsistent with how 'credit providers' and 'credit reporting bodies' (CRBs) determine missed repayments:

> [R]ather than requiring Credit Providers and CRBs to have to devise an alternative means of calculating missed payments (delinquency)…the definition [should] allow the inclusion of an indicator for whether the individual is up to date with their payments, and if not, an indicator of how long their oldest overdue payment has been outstanding.[97]

97 *Submission 27*, p. 13.

CHAPTER 4

Regulation of credit reporting

4.1 Proposed new Part IIIA, which inserts the new credit reporting provisions into the *Privacy Act 1988* (Privacy Act), is included in item 72 of Schedule 2 of the Bill. This chapter will examine some of the proposed credit reporting provisions referred to in submissions and evidence, including provisions that deal with:

- permitted disclosures of credit information by credit reporting bodies;
- use or disclosure of credit reporting information by credit reporting bodies for the purposes of direct marketing;
- use or disclosure of credit reporting information that is de-identified;
- correction of personal information by credit reporting bodies and credit providers;
- complaints procedures; and
- commencement of the credit reporting provisions.

Permitted disclosures by credit reporting bodies

4.2 Proposed new subsection 20E(1) of the Privacy Act prohibits a 'credit reporting body' which holds 'credit reporting information' about an individual from using or disclosing that information. The proposed section allows for some exceptions; however, the exceptions do not apply to 'credit reporting information' which is, or was, derived from 'repayment history information', unless the recipient of the information is a 'credit provider' who is the holder of an Australian Credit Licence under the *National Consumer Credit Protection Act 2009* (Cth) (National Consumer Credit Protection Act).[1]

4.3 According to the Explanatory Memorandum (EM):

> [I]t is considered appropriate that credit providers who cannot access repayment history information should not be able to indirectly obtain the benefit of that information through the possibility that credit reporting bodies could provide credit reporting information that incorporates repayment history information in another form.[2]

---

1 Proposed new subsection 20E(4) of the *Privacy Act 1988* (Privacy Act). Also see the Hon. Nicola Roxon MP, Attorney-General, *House of Representatives Hansard*, 23 May 2012, p. 5211.

2 Explanatory Memorandum (EM), pp 135-136.

'Repayment history information'

4.4 Some submitters argued, however, that the restriction will adversely affect their businesses. For example, Diners Club International (Diners Club) noted that, under regulation 62(1) of the National Consumer Credit Protection Regulations 2010, four expressly named charge card providers (including Diners Club) are exempt from the licensing requirements of the National Consumer Credit Protection Act:

> Diners Club would therefore be excluded from receiving or providing repayment history information either from or to a credit reporting agency; or from or to other credit providers, including its related bodies corporate. The current definition of the term "licensee" and its use in the revised Part IIIA means that Diners Club is at a competitive disadvantage against its major competitor in the charge card market, American Express Australia Limited (Amex Australia). As an issuer of credit cards and therefore a licensee, Amex Australia is able to obtain repayment history information about charge card applicants.[3]

4.5 Diners Club considered that it would be illogical to 'exclude charge card providers from the benefits of enhanced reporting' and suggested that charge card providers who are not licensees should have access to 'repayment history information'.[4]

4.6 The Communications Alliance recommended similarly that telecommunications providers, which are also not required to be licensed, should have the ability to opt into the regime:

> This way they would be able to provide a lead indicator to other financial service providers and it would also give the [telecommunications providers] a better understanding of a customer's capacity to pay before finalising the sale products and services to them.[5]

4.7 The Insurance Council of Australia (ICA) expressed concern that lenders mortgage insurers (LMIs) are not able to access 'repayment history information' directly from 'credit reporting bodies':

> As LMI providers take on the same risk as the lender, impeding their ability to assess this risk by denying direct access to the full range of credit information is likely to significantly affect the LMI providers' ability to actually provide LMI. This will impact on the availability and accessibility of borrowers (particularly first home buyers)...[D]irect access to all available credit information on a borrower is fundamental to the business model of a LMI provider.[6]

---

3 *Submission 28*, pp 1-2.

4 *Submission 28*, p. 2. The submission suggested two amendments to enable charge card providers to access repayment history information.

5 Mr John Stanton, Communications Alliance, *Committee Hansard*, 10 August 2012, p. 16. Mr Steven Brown, Dun & Bradstreet, *Committee Hansard*, 10 August 2012, p. 22, also endorsed this proposal.

6 *Submission 23*, p. 2.

4.8 The ICA contrasted the proposed restriction in new subsection 20E(4) with its ability to obtain 'repayment history information via a lender without being subject to a responsible lending obligation'.[7] Its submission called for consistency, recommending that proposed new subsection 20E(4) should be amended to read:

> (4) However, if the credit reporting information is, or was derived from, repayment history information about the individual, the credit reporting body must not disclose the information under paragraph (3)(a) or (f) unless the recipient of the information is a credit provider who is a licensee *or a mortgage insurer*.[8]

4.9 Min-it Software, the Consumer Credit Legal Service (WA) (CCLSWA) and the Consumer Credit Legal Centre (NSW) (CCLCNSW) opposed the inclusion of 'repayment history information' in the credit reporting provisions. CCLCNSW, for example, recommended that this information be removed from the Bill for a number of reasons, including:

> It won't always lead to more responsible lending decisions.
>
> It has the potential to entrench hardship.
>
> Credit providers have alternative methods of accessing repayment history information, and there is no evidence to suggest that the absence of repayment history is causing significant problems in the market, therefore its inclusion is not justified from the privacy perspective.
>
> It will lead to more risk-based pricing, which will entrench disadvantage.[9]

4.10 At the first public hearing, Ms Katherine Lane from the CCLCNSW explained further:

> The main reason that the credit providers need this information is so that they can deal with managing risk and pricing risk, and that does not necessarily get a positive outcome for consumers. Pricing risk is about interest rates. I think the main outcome is going to be that you will have some little dots or marks on your report and then they will charge you extra interest…It is also an intrusion on [an individual's] privacy for something that is going to be to their detriment overall.[10]

4.11 Min-it Software argued that the inclusion of 'repayment history information' in the Bill conflicts with proposed Australian Privacy Principle 3 (Collection of solicited personal information):

> [T]he reporting of such information to a credit reporting business is not a necessary function nor one reasonably necessary for the credit provider to perform its responsible lending or other credit activities. It is also not reasonably necessary, though it might be convenient from a commercial

---

7 *Submission 23*, Attachment 1, p. 3.

8 *Submission 23*, Attachment 1, p. 9 (emphasis in original).

9 *Submission 51*, p. 5. The submission details each of these arguments: see pp 6-13.

10 *Committee Hansard*, 10 August 2012, p. 30.

> practice perspective, for another credit provider to see such history where that credit provider uses or is provided with a scoring mechanism supplied by the credit reporting business.[11]

More comprehensive credit reporting – general comments

4.12 'Repayment history information' is one of five new data sets being introduced into the credit reporting system as a move toward more comprehensive, or positive, credit reporting, as recommended by the Australian Law Reform Commission (ALRC).[12] The other four data sets are: the date on which a credit account was opened; the date on which a credit account was closed; the type of credit account opened; and the current limit of each open credit account.[13]

4.13 According to the Explanatory Memorandum (EM):

> Comprehensive credit reporting will give credit providers access to additional personal information to assist them in establishing an individual's credit worthiness. The additional personal information will allow credit providers to make a more robust assessment of credit risk and assist credit providers to meet their responsible lending obligations. It is expected that this will lead to decreased levels of over-indebtedness and lower credit default rates. More comprehensive credit reporting is also expected to improve competition and efficiency in the credit market, which may result in reductions to the cost of credit for individuals.[14]

4.14 Some submitters and witnesses commented generally in relation to this reform. Veda, Dun & Bradstreet and Experian, among others, supported the introduction of positive credit reporting to facilitate risk assessment and compliance with responsible lending obligations.[15] Veda particularly noted the preliminary

---

11 *Submission 48*, p. 11. Also see the Consumer Credit Legal Service (WA), which argued that the inclusion of 'repayment history information' in the Bill would be invasive and beyond what is reasonably necessary for 'credit providers' to assess an individual's credit worthiness: *Submission 6*, pp 2 and 4.

12 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 1. Also see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Recommendations 55-1 to 55-3.

13 EM, p. 3.

14 EM, p. 3.

15 Mr Steven Brown, Dun & Bradstreet, *Committee Hansard*, 10 August 2012, p. 22; Ms Sharon Booth, Experian, *Committee Hansard*, 10 August 2012, p. 21. Also see, for example, Insurance Council of Australia, *Submission 23*, p. 2; Mr Timothy Pilgrim, Australian Privacy Commissioner, *Committee Hansard*, 10 August 2012, p. 8; Mr Damian Paull, Australasian Retail Credit Association, *Committee Hansard*, 10 August 2012, p. 14; Mrs Sue Jeffrey, ANZ Banking Group Limited, *Committee Hansard*, 10 August 2012, p. 15.

findings of its current Comprehensive Reporting Pilot Study[16] and, in evidence, Mr Steven Brown from Dun & Bradstreet argued that the Bill should go further:

> [W]e support the model that has been put forward. It does provide much more balance…[H]owever,…we feel we have stopped a little short of the opportunity here—that is, somebody who has a default on their file yet is meeting payments to utility companies and telecommunications companies will not have that information recorded on their file or will not have the option to have that data recorded on their file by those organisations… There are scenarios today where individuals are not able to establish a track record of payment to a financial services provider but may well have those facilities being kept in good order. The ability to include that information on the credit file would indeed allow those individuals to have that good payment performance reflect on their file, notwithstanding that they may have one negative incident on their file. So that is really the issue of fairness that I am referring to, trying to get more balance into the system.[17]

4.15 However, some submitters – such as the CCLSWA and the Australian Privacy Foundation (Privacy Foundation) – contended that positive credit reporting will not advantage consumers. The CCLSWA, for example, rejected the argument that the inclusion of the five additional data sets in the credit reporting system will improve the system's efficiency, decrease over-indebtedness and open up competition:

> On the contrary, studies have indicated that there is no correlation between positive credit reporting and reduced levels of indebtedness. Nor is there necessarily a correlation between positive reporting and responsible lending practices….It seems more likely that the reliance on repayment history information will lead to a rise in the number of consumers being unfairly refused credit where there are no adverse file listings, and their loan applications would otherwise be approved.[18]

4.16 The Privacy Foundation argued:

> We welcome the imposition of responsible lending conditions for participation in the credit reporting provisions, which protects consumers against the more blatant irresponsible lending practices, but this does not mean that consumer vulnerabilities will not be exploited to provide credit which is not in the consumer's best interests.[19]

---

16 Additional information, tabled 10 August 2012. The Australasian Retail Credit Association similarly referred to research published by the United States-based Policy and Economic Research Council: 'Credit Impact of More Comprehensive Credit Reporting in Australia and New Zealand', August 2012, available at: http://perc.net/files/PERC%20Report%20-%20Final.pdf (accessed 20 August 2012).

17 *Committee Hansard*, 10 August 2012, pp 26-27.

18 *Submission 6*, pp 2-3. For similar comments, also see Consumer Credit Legal Centre (NSW), *Submission 51*, pp 5-13.

19 *Submission 49*, p. 23.

Departmental response

4.17 In response, the Attorney-General's Department (Department) referred to the Regulation Impact Statement (RIS) accompanying the Bill, which identifies the potential risks and benefits of including 'repayment history information' as a fifth data set in the credit reporting system. The RIS concludes, on balance, that 'repayment history information' should be included in the credit reporting system.[20]

4.18 The Department noted that the consumer protections recommended by the ALRC have been incorporated into the Bill:

> The Department does not consider that any additional legislative measures in the Privacy Amendment Bill would resolve the disagreement between stakeholders on the possible implications of including repayment history information in the credit reporting system.[21]

Use or disclosure of credit reporting information by credit reporting bodies for the purposes of direct marketing

4.19 According to the EM:

> Pre-screening is a direct marketing process by which direct marketing credit offers to individuals are screened against limited categories of credit information about those individuals to remove individuals from the direct marketing credit offer, based on criteria established by the credit provider making the offer, before the offers are sent. Generally, the process for pre-screening a direct marketing credit offer works as follows. The credit provider making the credit offer establishes the eligibility requirements for the direct marketing credit offer and provides the list of individuals about whom the pre-screening assessment will be made; the credit reporting body undertakes the pre-screening assessment and determines whether an individual is eligible consistent with those criteria; the credit reporting body discloses the pre-screening assessment to a mailing house which conducts the direct marketing consistent with the pre-screening assessment, and then the pre-screening assessment is destroyed by the credit reporting body and the mailing house.[22]

General prohibition

4.20 Proposed new subsection 20G(1) of the Privacy Act prohibits a 'credit reporting body' which holds 'credit reporting information' about an individual from using or disclosing the information for direct marketing purposes. The prohibition does not apply to the use by the 'credit reporting body' of 'credit information' about an individual for direct marketing purposes by, or on behalf of, a credit provider (pre-screening), subject to certain conditions (proposed new subsection 20G(2) of the Privacy Act).

---

20 EM, p. 29.

21 Additional information, received 29 August 2012, p. 7.

22 EM, p. 138 (emphasis in the original).

4.21 Some submitters supported the proposed prohibition, with a few submissions recommending amendments to enhance the operation of the provision.[23] The CCLCNSW, for example, submitted that the permitted use for pre-screening should be removed from the Bill:

> [T]he use of credit reporting information to facilitate pre-screening is an unnecessary breach of privacy. It is abhorrent to use the credit reporting system for marketing…[D]irect marketing and pre-screening should be prohibited…[T]he utility of pre-screening should be reviewed in light of the recent amendments to the National Consumer Credit Protection Act on unsolicited offers of credit. The Act now specifically prohibits unsolicited offers of credit unless the consumer has opted in. It is our understanding that many consumers have not chosen to opt-in. In these circumstances, the need for pre-screening advocated by industry is now considerably less.[24]

4.22 In 2008, the ALRC recommended that the new Privacy (Credit Reporting Information) Regulations should prohibit the use or disclosure of 'credit reporting information' for direct marketing purposes, including the pre-screening of direct marketing lists.[25] However, the Australian Government responded:

> …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.[26]

Opt-out mechanism

4.23 Proposed new subsection 20G(5) provides an 'opt-out' mechanism, allowing an individual to request a 'credit reporting body' that holds 'credit information' about the individual not to use that information for pre-screening purposes. The Privacy Foundation questioned the practicality of this provision given the lack of a direct relationship between the individual and a 'credit reporting body' (CRB):

> [I]t is unrealistic to rely on individuals 'finding' a CRB to opt-out – they must be given the opportunity via their direct relationship with a Credit Provider.[27]

---

23 For example, Australasian Retail Credit Association, *Submission 27*, p. 15; and Australian Privacy Foundation, which argued further that pre-screening should only apply to 'negative information' such as default information and serious credit infringements: see *Submission 49*, p. 29.

24 *Submission 51*, pp 16-17.

25 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Recommendation 57-3.

26 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, p. 116.

27 *Submission 49*, p. 28. The submission states that this would be consistent with the *Do Not Call Register Act 2006* and the *Spam Act 2003*.

4.24 The Law Council of Australia added that the Bill does not explain the consequences of an 'opt-out' request:

> A more practical measure may be for a credit reporting agency (or perhaps all credit reporting agencies) to establish a separate database of pre-screening opt-out individuals. All customer lists for which pre-screening had been requested would initially be "washed" against this opt-out list and the opted-out persons removed from the prospects list, before any use was made of credit information referred to in clause 20G(2). It should be expressed in proposed section 20G that an opted out person would not receive the credit offer proposed to be offered to persons who are successfully screened.[28]

4.25 The Australian Bankers' Association (ABA) and the Australasian Retail Credit Association (ARCA) referred to one of the conditions giving rise to a permitted use: the information cannot be 'consumer credit liability information' or 'repayment history information' about an individual.[29] These submitters recommended that the condition be clarified to expressly cover both direct and indirect use of information in a pre-screening process. As highlighted in the ABA's submission:

> Indirect use means using the new data sets as model inputs to derive an outcome. For example, a credit reporting agency may blend the data sets into a model to derive a credit propensity score that predicts a customer's likelihood to be receptive to an offer of credit. This predictor could then be used for pre-screening or direct marketing.[30]

Use or disclosure of credit reporting information that is de-identified

4.26 Proposed new subsection 20M(1) of the Privacy Act prohibits a 'credit reporting body' which holds de-identified 'credit reporting information' (de-identified information) from using or disclosing that information. The general prohibition does not apply if the use or disclosure is for the purposes of conducting research in relation to the assessment of the credit worthiness of individuals and the 'credit reporting body' complies with any rules made by the Australian Information Commissioner (Commissioner) (proposed new subsection 20M(2) of the Privacy Act).

4.27 The EM states that the purpose of regulating de-identified information is to clarify that such information can be used or disclosed in specific circumstances:

> [I]nformation from the credit reporting system has in the past been used for the purpose of conducting research (including statistical modelling and data analysis) relating to the assessment or management of credit. This research, where it is in the public interest, should be expressly permitted. Conducting research with de-identified personal information enhances privacy

---

28 *Submission 14*, p. 13. The Law Council of Australia also submitted that it would be preferable to expressly include a statement that no written record must be made of an opted-out individual being removed from a marketing list and no communication of a consumer's opted-out status should be made to the credit provider or their agent.

29 Proposed new paragraph 20G(2)(c) of the Privacy Act.

30 *Submission 24*, p. 7. Also see Australasian Retail Credit Association, *Submission 27*, pp 15-16.

> protection and appears to be consistent with existing industry practices. In addition, research is not a primary purpose of the credit reporting system and it is not appropriate to allow credit reporting information that identifies individuals to be used for research purposes.[31]

4.28 The EM notes, however:

> [T]here can be concerns about the effectiveness of methods used to de-identify personal information and the risks of that information subsequently being linked again to individuals in a way that allows them to be identified.[32]

Suggestions to remove proposed new section 20M

4.29 Some submitters questioned the appropriateness of regulating de-identified information. These submitters argued that once 'credit reporting information' has been de-identified, it is no longer personal information about an individual within the scope of the Privacy Act. These submitters suggested that proposed new section 20M of the Privacy Act should be removed from the Bill.[33] For example, ARCA recommended:

> [T]he Government remove [proposed new section] 20M from the Bill entirely, and refer the question of the economic value of depersonalised data to the Productivity Commission for inquiry. Such an inquiry is likely to provide a range of reforms for the Government to consider in relation to the regulation of this important economic tool.[34]

4.30 Veda also objected strenuously to the regulation of de-identified data in the Privacy Act and supported retaining the purpose for which de-identified data may be used without prescribing rules (including those which might be made by the Commissioner).[35]

4.31 Submitters and witnesses from the finance and credit industries indicated that they could not understand the rationale behind proposed new section 20M of the Privacy Act. In detailed submissions, these stakeholders described the fundamental role of de-identified information in the information economy.[36] For example, Dun & Bradstreet, Experian and Veda jointly submitted:

> The information economy revolves around research using de-personalised information. Before parliament decides to restrict one part of the

---

31 EM, p. 144.

32 EM, p. 144.

33 For example, see: ANZ Banking Group Limited, *Submission 29*, p. 8; Experian, *Submission 35*, p. 5; Mr Steven Brown, Dun & Bradstreet, *Committee Hansard*, 10 August 2012, p. 22.

34 *Submission 27*, p. 7.

35 *Submission 41*, p. 3.

36 For example, Australasian Retail Credit Association, *Submission 27*, p. 7; ANZ Bank, *Submission 29*, p. 8; Veda, *Submission 41*, pp 1 and 4-7.

> information economy from using de-personalise[d] data, industry believes it appropriate to consider the value and role that research brings.[37]

4.32 In evidence, Professor Les McCrimmon distinguished credit-reporting information from the re-identification of health information for the purposes of research and statistical data sets:

> [I]t is a live issue in relation to health research, because in health research there is often the master key and the need to re-identify to check the research and the research findings. That does not arise in a credit-reporting context and…there has not been an occasion in the 40 years that it has been operating for the requirement to re-identify.
>
> …
>
> To go back to basic principles, the Privacy Act is primarily concerned with protecting personal privacy, namely personal information, as part of implementing Australia's obligations under the International Covenant on Civil and Political Rights. When the information is no longer personal information, the work of the Privacy Act should end. To extend the work of the Privacy Act beyond personal information to de-identified information, which by definition is not personal information, has a couple of problems. One is that it puts an obligation on the Office of the Information Commissioner to come up with rules to regulate what in the past has never been regulated and, across privacy regimes in all [Organisation for Economic Co-operation and Development] countries, is not regulated for a good reason: it is not personal information; it does not impact on the human right—namely the protection of privacy. So that is the first problem.[38]

4.33 Professor McCrimmon did not consider the re-identification of data to be a problem in the credit reporting context;[39] nor did Ms Kim Jenkins from Experian, who argued:

> There is no purpose behind re-identification in the credit industry. De-identified information is for the purpose of scorecards, and that has to be done on a depersonalised, anonymous basis in order for the underlying statistical modelling to be valid and robust, and then there is no purpose in repersonalising that, because that scorecard goes into production. There is no benefit in relinking it to individuals.[40]

4.34 ARCA suggested that the better legislative approach would be to prohibit the re-identification of data,[41] a view with which the three main credit reporting agencies

---

37 *Submission 44*, p. 2.

38 *Committee Hansard*, 10 August 2012, p. 24.

39 *Committee Hansard*, 10 August 2012, p. 24.

40 *Committee Hansard*, 10 August 2012, p. 25. For similar comments, see Mr Steven Brown, Dun & Bradstreet, *Committee Hansard*, 10 August 2012, p. 25.

41 *Submission 27*, p. 7.

(to be renamed 'credit reporting bodies' by the Bill) agreed.[42] Veda suggested further that the Bill should appropriately penalise the re-personalisation of data:

> [I]t is prudent to recommend the inclusion in the legislation of substantial penalties for subsequent re-personalisation with substantial penalty provisions as apply elsewhere in the Bill.[43]

4.35 Professor McCrimmon agreed that 'the better policy way to deal with [this issue] is to penalise re-identification rather than put a blanket ban on the use of de-identified data'.[44]

History of proposed new section 20M

4.36 In 2008, the ALRC examined the issue of the use and disclosure of 'credit reporting information' for secondary purposes (such as research). The ALRC concluded:

> 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.[45]

4.37 The Australian Government did not accept this recommendation 'as it would allow credit reporting information to be used and disclosed for a number of unknown purposes'. The government acknowledged:

> [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.
>
> [T]he Government will…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.[46]

4.38 In 2010-2011, the Senate Finance and Public Administration Legislation Committee (F&PA committee) reported on the Exposure Drafts of the Bill, including

---

42 Dun & Bradstreet, Experian and Veda, *Submission 44*, p. 2.

43 *Submission 41*, p. 9. Also see Dun & Bradstreet, Experian and Veda, *Submission 44*, p. 2.

44 *Committee Hansard*, 10 August 2012, p. 24.

45 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Recommendation 57-2.

46 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, p. 116.

the pre-cursor to proposed new section 20M.[47] The F&PA committee noted, among other things, a suggestion from the Office of the Australian Information Commissioner (OAIC) that the provision did not permit the disclosure of de-identified information and was not clear in relation to whether the related rules to be issued by the OAIC must be in place before any research is permitted.[48] The F&PA committee recommended that these issues be addressed.[49] The Australian Government accepted and implemented the recommendations of the F&PA committee,[50] particularly in proposed new paragraph 20M(2)(b) of the Privacy Act to provide that a 'credit reporting body' must comply with rules made by the Commissioner under proposed new subsection 20M(3).[51]

Departmental response

4.39 In evidence to the current inquiry, an officer from the Department reiterated the government's view expressed in the EM regarding the potential re-identification of data, as well as the issue of 'what is discernible from the characteristics of the data that is de-identified that can lead one to identification'.[52] Further:

> The credit reporting scheme is set up…on the basis that basically everything is prohibited and then there are a series of exceptions to say, 'This is how entities may deal with this type of data.' So the rules around the de-identified data is to say that we need to put some rules around this type of secondary use, which is to de-identify and then to do research with the data.[53]

4.40 In additional information provided to the committee, the Department clearly advised:

> The purpose of clause 20M is to ensure that the Information Commissioner has the power to issue appropriate guidelines to deal with how an individual's personal financial information may be used for research.[54]

---

47 Clause 115 of the Exposure Draft Bill.

48 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 111.

49 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 113 (Recommendation 16).

50 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Draft of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 8.

51 See subclause 115(2) of the Exposure Draft Bill.

52 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 14.

53 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 14.

54 Additional information, received 29 August 2012, p. 9.

Correction of personal information by credit reporting bodies and credit providers

4.41 Proposed new sections 20T and 21V of the Privacy Act respectively enable an individual to request a 'credit reporting body' or 'credit provider' to correct certain types of personal information about the individual.

4.42 The EM states:

> Importantly, individuals are able to request the correction of their personal information that may not be held by the credit reporting body, requiring the credit reporting body to consult with the appropriate credit reporting body or credit provider. This imposes a specific obligation on bodies and credit providers to assist individuals to correct their personal information, no matter whom it is held by in the credit reporting system. This means that the credit reporting body or credit provider to which the individual first makes a correction request must deal with that request and assist the individual to have their personal information corrected.[55]

Third party application

4.43 Some submitters expressed concern with the potential need for an entity which receives a complaint to consult with another entity. For example, ARCA submitted:

> [T]he Bill suggests that the first party contacted (the respondent) must undertake (presumably themselves) to notify 'everyone' who has received the disputed information, collate the necessary information to respond to the complaint, and then respond on behalf of all relevant parties. What seems to be a simple requirement under the Bill becomes complex because of the degree of prescription of how an operational process must work, rather than simple articulation of the outcome that it seeks to deliver.
>
> To manage consumer complaints effectively, it is essential for relevant parties to manage and resolve the complaint wherever possible. However, the first point of contact may not always be best placed to manage a complaint. It may be more appropriate to refer the consumer to the most appropriate respondent.[56]

4.44 The OAIC was similarly concerned with how an individual is able to correct personal information not held by the party who is first contacted. The OAIC's submission emphasised the need for clear, appropriate and comprehensive correction and notification obligations:

> [I]t is important that the Bill clearly sets out:
>
> - the obligation on the entity that received the correction request to take reasonable steps to have the information corrected

---

55 EM, pp 148-149. In relation to proposed new subsection 20T(1), see EM, p. 180.

56 *Submission 27*, p. 11. The Australasian Retail Credit Association highlighted that the definition of the term 'credit provider' could result, for example, in an entity that has no affiliation with the credit reporting system being compelled to resolve credit reporting issues: see pp 9-10.

> - the obligation on the entity that holds the information to correct that information
>
> - the obligation on the entity that received the correction request to notify the individual about the outcome of their correction request.
>
> There is uncertainty as to whether the provisions in the Bill achieve this…The OAIC…recommends that the Bill be amended to ensure that the correction provisions are clear, and operate effectively.[57]

Breadth of request to correct

4.45 Other submitters focussed on specific issues, including: the types of personal information captured by the proposed provisions; the time allowed for the correction of personal information; and incorrect or unfair listings.

4.46 The types of personal information in respect of which an individual can request a correction are:

- 'credit information' about the individual;
- 'CRB derived information' about the individual; and
- 'CP derived information' about the individual.

4.47 The ANZ Banking Group Limited (ANZ), for example, submitted that 'CRB derived information' and 'CP derived information' are assessments of an individual's credit worthiness. In its view, individuals should not be entitled to amend such an assessment.[58] The Australian Finance Conference (AFC) argued similarly that evaluative information generated by an APP entity in a commercially sensitive decision-making process should not be correctable:

> The omission potentially invites opening a credit provider to risk of fraud or customer manipulation of credit application data should the credit provider be obliged to reveal commercially sensitive components of its lending decisioning process.[59]

Time to correct and substantiation

4.48 Proposed new subsections 20T(2) and 21V(2) of the Privacy Act require a 'credit reporting body' or 'credit provider', if satisfied that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading, to take reasonable steps to correct the information within 30 days or a longer period agreed to in writing by an individual.

4.49 The Energy & Water Ombudsman NSW (EWON) described the 30-day timeframe allowed for the correction of personal information as 'excessive':

---

57 *Submission 47*, pp 23-24.

58 *Submission 29*, pp 7-8. Also see Australasian Retail Credit Association, which agreed, but queried how a consumer is to determine whether 'CP derived information' is correct: *Submission 27*, p. 15.

59 *Submission 36*, p. 9.

> If there is a valid reason for the delay, we suggest that the credit reporting agency makes an annotation to the file to note that a correction is pending.[60]

4.50 The Telecommunications Industry Ombudsman agreed that the timely removal of incorrect information is critical:

> In our view, a period of 30 days to correct information on a credit file is too long when it may have the potential to compound difficulties experienced by consumers, particularly where they need to apply for finance and where incorrect information on their credit file is impeding them from doing so. The Telecommunications Consumer Protection (TCP) Code requires that where a telephone or internet company becomes aware that their customer has been default listed in error, they must inform the ['credit reporting body'] within one (1) working day.[61]

4.51 Conversely, the Australian Privacy Commissioner, Mr Timothy Pilgrim, told the committee that when listings are disputed 'it requires on a number of occasions a bit more time than [30 days] to be able to get the facts together to support whether there has been a default or not'.[62]

4.52 The Privacy Foundation contended that the 30-day timeframe specified in proposed new subsection 20T(2) is 'weaker' than the ALRC Recommendation 59-8.[63] The ALRC's recommendation was for the new Privacy (Credit Reporting Information) Regulations to:

> …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.[64]

4.53 In relation to substantiation, CCLCNSW argued that it is essential for a 'credit provider' to be able to produce evidence verifying the accuracy of a listing:

---

60 *Submission 38*, p. 5. The Energy & Water Ombudsman (NSW) added that, read in conjunction with the proposed new complaints provisions (particularly proposed new paragraph 23B(5)(a) of the Privacy Act), an individual might have to wait up to 60 days before being able to engage in external dispute resolution or approach the Australian Information Commissioner. Also see Australian Privacy Foundation, which argued that industry should devise a means of flagging corrected or disputed information: see *Submission 49*, p. 31.

61 *Submission 45*, p. 7.

62 *Committee Hansard*, 21 August 2012, p. 9.

63 *Submission 49*, p. 31.

64 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, p. 69 (Recommendation 58-9). This recommendation was accepted by the Australian Government: see 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, p. 128.

> The credit reporting system operates on an "honour basis", that is, credit providers are trusted and there are no checks on reported information. To balance this, consumers must be able to reasonably insist that this information be verified.[65]

4.54 Consistent with ALRC Recommendation 59-8, but with reference to the Privacy Act (and not the regulations), CCLCNSW recommended that proposed new section 20T should be amended to require a 'credit reporting body' to request evidence of a disputed listing from a 'credit provider' and, if not provided within 30 days of the request, the 'credit reporting body' must remove the disputed listing.[66]

Departmental response

4.55 In evidence, a departmental officer agreed that the Australian Government had accepted ALRC Recommendation 59-8, but explained that the way in which that recommendation has been implemented in the Bill is slightly different from the way in which the government response was framed:

> Essentially, if there is a request to correct and that request is denied, the credit provider has to substantiate the reason for doing so, so they have to provide you with the evidence. There is no express provision saying that if they cannot substantiate they must change, because the general obligation to keep accurate records will apply anyway. So if they cannot provide an individual with the evidence to show why the listing is there then there is no evidence for the listing. Therefore the general obligation to keep accurate, up-to-date records would apply, and they should be updating their records.[67]

Concept of fairness

4.56 CCLCNSW submitted that another major problem for consumers is default listings, or repayment history listings, in circumstances where a reasonable person would consider the listing to be unfair:

> There are a number of circumstances where the consumer is unable to pay because of matters arising that are completely out of their control. Some examples are:
>
> 1. Natural disasters
>
> 2. Bank error in processing a direct debit or Bpay
>
> 3. Fraud
>
> 4. Illness and hospitalisation

---

65 *Submission 51*, p. 18.

66 *Submission 51*, p. 18.

67 Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 9. Also see Senate Finance and Public Administration Legislation Committee, *Exposure Draft of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 94 (Recommendation 14); Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Draft of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 7.

> 5. Mail theft
>
> It is essential that consumers have access to a mechanism to challenge a listing on the grounds of fairness.[68]

4.57 The CCLCNSW recommended that proposed new section 21V should be amended to enable consumers to request correction of a listing on the grounds that it would be unfair and misleading in the circumstances for the listing to remain uncorrected.[69]

Departmental response

4.58 In evidence, a representative from the Department emphasised that the inability to contact an individual, can give rise to a 'serious credit infringements' but was not certain that was likely to happen in the circumstances described by the CCLCNSW (due to the enhanced contact requirement).[70]

4.59 In any event:

> The Department is not able to express a view on whether a credit provider should list a serious credit infringement in circumstances where an individual has suffered the consequences of a natural disaster. However, the Department notes that the definition of serious credit infringement requires the credit provider to be satisfied that a reasonable person would consider the individual's act (for example, of missing one or more payments because of a natural disaster) indicates an intention to no longer comply with the individual's obligations.[71]

External dispute resolution schemes

4.60 Proposed new section 21W of the Privacy Act requires a 'credit provider' to give an individual written notice, within a reasonable period, of the outcome of their request for the correction of personal information under proposed new section 21V. In particular, if the personal information has not been corrected, the written notice must state that the correction has not been made; set out the reasons for the 'credit provider' not correcting the information (including evidence substantiating the correctness of the information); and:

> (c) state that, if the individual is not satisfied with the response to the request, the individual may:
>
> (i) access a recognised external dispute resolution scheme of which the provider is a member; or
>
> (ii) make a complaint to the Commissioner under Part V.

---

68 *Submission 51*, p. 18.

69 *Submission 51*, p. 18.

70 Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 10.

71 Answer to question on notice, received 3 September 2012, p. 16.

4.61 Proposed new section 21W is one example of a provision in the Bill which enables an individual to progress an unresolved dispute through either a recognised external dispute resolution (EDR) scheme or the Commissioner. The proposed complaints provisions – such as proposed new paragraph 23B(4)(b) – contain a similar mechanism.

4.62 Min-it Software expressed concern with these provisions which, it argued, considerably enhance the existing EDR providers' involvement in privacy complaints:

> We do not believe that it is appropriate to give the two private companies (which are not statutory authorities) engaged in providing EDR for credit even greater power than they currently have, particularly at the expense of direct contact with the Privacy Commission[er].[72]

4.63 In relation to the recognition of EDR schemes for the purposes of the Privacy Act, Mr Pilgrim advised that he has not yet made any assessments but will begin to consider the matter once the Bill has been enacted.[73] However:

> [T]here is a range of criteria that I would need to take into account before approving a scheme to operate as an EDR scheme under the [A]ct. A number of those areas go into some fairly obvious ones, but one of them is the independence of the scheme and its ability to operate independently. I would have to be satisfied before approving an EDR scheme to participate that it met that criterion.[74]

4.64 One other concern – expressed in the Energy & Water Ombudsman NSW's (EWON) submission regarding proposed new sub-paragraph 21W(3)(c)(i) – was that the EDR provisions could inadvertently result in customer referral to the wrong EDR scheme for a particular issue:

> For example, a customer may contact their financial institution to dispute their credit listing and the credit listing may be for an old energy debt. If after investigation the financial institution is unable to assist the customer[,] 21W(3)(c)(i) suggests that they must be referred to the 'external dispute resolution scheme of which the provider is a member', so the referral would be to the Financial Ombudsman Service, of which the provider is a member. However, as the customer is disputing a listing related to an energy debt the most appropriate external dispute resolution scheme would be EWON.[75]

---

72 *Submission 48*, p. 9.

73 *Committee Hansard*, 21 August 2012, pp 10-11.

74 *Committee Hansard*, 21 August 2012, p. 12.

75 *Submission 38*, p. 6. Also see Australian Bankers' Association, answer to question on notice, received 30 August 2012, p. 3.

Complaints procedures

4.65 Division 5 of new Part IIIA of the Privacy Act sets out provisions in relation to complaints. Proposed new section 23A gives individuals the right to complain to 'credit reporting bodies' or 'credit providers' about acts or practices that might be a breach of the credit reporting provisions or the registered credit reporting code (to be created by Schedule 3 of the Bill).

4.66 Proposed new section 23B sets out how 'credit reporting bodies' and 'credit providers' are to deal with those complaints. For example, proposed new subsection 23B(1) provides that the respondent to a complaint:

> (a) must, within 7 days after the complaint is made, give the individual a written notice that:
>
> (i) acknowledges the making of the complaint; and
>
> (ii) sets out how the respondent will deal with the complaint; and
>
> (b) must investigate the complaint.

Notification provisions

4.67 Several submissions addressed proposed new section 23B of the Privacy Act, with some questioning the notification requirements in proposed new paragraph 23B(1)(a). For example, the Australasian Retail Credit Association submitted that the majority of complaints are resolved within 48 hours and compliance with that provision would be 'unnecessary, wasteful and irritating for the consumer'. Further:

> [I]t should be acceptable for other methods of communication to be allowed on the basis that a formal record is retained, such as a file note made in a customer relationship/complaints management system, or tape recording of voice communications.[76]

4.68 The Communications Alliance agreed with the need for a less prescriptive form of communication, submitting that most telecommunications customers prefer to deal with their telecommunications providers via telephone or email, and increasingly via social media – such as on Twitter or Facebook.[77] Optus commented similarly:

> [W]e are concerned that the prescriptive complaint handling requirements set out in the Bill (such as the requirement for written acknowledgement of complaints and then written confirmation of the outcomes of complaints) are very rigid and reflect an out-dated method of interacting with customers. Such restrictive practices do not take into account the multitude of ways in which customers are able to contact their providers in the digital environment.[78]

---

76 *Submission 27*, p. 11.

77 *Submission 30*, p. 7.

78 *Submission 31*, p. 5. For similar comments, also see Telecommunications Industry Ombudsman, *Submission 45*, pp 8-9.

Third party issues

4.69 Some submitters were also concerned by proposed new subsection 23B(2), which will require the respondent to the complaint to consult another 'credit reporting body' or 'credit provider' about the complaint, if the respondent considers that consultation to be necessary. As with the correction of personal information, third party issues concerned some submitters – for example, the Financial Ombudsman Service (FOS), the Consumer Action Law Centre (CALC), and ARCA.

4.70 The FOS considered that the regime will prove impractical as many complaints will relate to a financial services provider ('Bank A') holding incorrect personal information which it may have obtained from another body (for example, 'Energy Provider B'):

> Bank A enquires as to the accuracy of that information from Energy Provider B and is told that the information is correct. The complainant is unhappy with the response and takes the matter to Bank A's EDR scheme. Energy Provider B is not a member of that EDR Scheme. In those circumstances the EDR Scheme will not be able to properly investigate the dispute as it will be unable to access the relevant information which is held by Energy Provider B, and by its member Bank A. All Bank A's EDR scheme will be able to do is consider if Bank A has followed an appropriate process in dealing with the request, but it will not be able to solve the consumer's main problem, which is correcting any wrong information at its source.[79]

4.71 For this reason, FOS, EWON and the Telecommunications Industry Ombudsman supported redrafting proposed new section 23B to allow a consumer to be referred to the appropriate EDR scheme by the first respondent to the complaint.[80]

4.72 ARCA submitted that the complaints-handling processes in the Bill:

> …will require a complex system to be developed between the multitude of Credit Providers and CRBs who use the credit reporting system to manage the finalisation of consumer complaints. Such a system would increase the risk of inadvertent disclosure, remove the ability of the consumer to deal directly with the cause of the complaint, and is against industry practice and good business practice regarding customer service.[81]

4.73 ARCA's Chief Executive Officer, Mr Damian Paull noted further:

> The complexity of the proposed arrangements will inevitably lead to delay and unnecessary escalation to alternative dispute arrangements, creating further financial burden on credit providers through EDR scheme fees;

---

79 *Submission 12*, p. 7. For similar comments, also see Energy & Water Ombudsman NSW, *Submission 38*, p. 7.

80 *Submission 12*, p. 7, *Submission 38*, p. 7 and *Submission 45*, p. 9, respectively. Also see Communications Alliance, answer to question on notice, received 23 August 2012, p. 2.

81 *Submission 27*, p. 12.

> increased resourcing requirements for the OAIC, the regulator; and, most importantly, delayed consumer outcomes.[82]

4.74 ARCA and Experian recommended that the Bill should allow the respondent to the complaint to be able to refer a consumer to the entity which is most able to resolve the complaint, backed by oversight from the regulator.[83]

4.75 The Consumer Action Law Centre (CALC) supported proposed new section 23B of the Privacy Act:

> [I]t aims to prevent credit providers and credit reporting agencies buck-passing complaints between themselves (which has been a big problem to date) and limits the risk of consumers dropping out of the complaints process because they do not know where to complain.[84]

4.76 Despite this, the CALC considered that the provision might be too broad and could capture third parties who are reluctant to assist in the resolution of a complaint:

> [T]he obligation to resolve a complaint should lie with the first party to be contacted by the consumer which is actually involved in the subject of the complaint. This would usually be the relevant credit reporting agency, or the credit provider which made the listing. However, to ensure that consumers don't 'fall through the cracks', a credit provider or credit reporting agency which did not have any role in the subject of the complaint, should have an obligation to advise the consumer of the parties which could deal with the dispute.[85]

4.77 In evidence, a departmental officer told the committee that the corrections and complaints processes have been re-designed to make them simpler:

> In the correction process, the approach taken is that, if a person requests a correction, they make the request once to a credit provider or a credit reporting body, and they have the obligation of consulting with other industry members to resolve the issue. So you are not bounced around… That is the intention in relation to the correction process. The recipient of a complaint can refuse the complaint if it is not about them…If I am making a complaint—if I say to them, 'You've disclosed information in the wrong way'—then that is about their act or practice in relation to the information, so I have to complain to the right person who did the wrong thing, essentially. So they can transfer my complaint to someone else but they cannot transfer my correction request.[86]

---

82 *Committee Hansard*, 10 August 2012, p. 14.

83 *Submission 27*, p. 12.

84 *Submission 5*, p. 6.

85 *Submission 5*, p. 7. For similar comments, also see Australian Finance Conference, *Submission 36*, p. 9.

86 Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 15.

Industry regimes

4.78 Submitters were also concerned with jurisdictional issues raised by proposed new section 23B of the Privacy Act. The Communications Alliance, for example, submitted that the Bill does not recognise long-established credit-related regulations in several industries,[87] including: the Communications Alliance Telecommunications Consumer Protections Industry Code and Telecommunications Industry Ombudsman Scheme (in relation to the communications industry);[88] *Regulatory Guide 165: Licensing: Internal and external dispute resolution* (RG 165) (in relation to licensees under the National Consumer Credit Protection Act);[89] and AS ISO 10002-2006.[90]

4.79 The Communications Alliance argued that the Bill imposes new obligations, which conflict with standard practices in those industries, potentially leading to consumer confusion and inconsistent approaches.[91] One such conflict, noted in submissions from ARCA and ANZ, arises from the prescriptive timeframes in proposed new subsections 23B(4) and 23B(5) of the Privacy Act.

4.80 Proposed new subsections 23B(4) and 23B(5) of the Privacy Act require the respondent to a complaint, after investigation and within 30 days, to make a decision about the complaint and give the individual who made the complaint written notice of the respondent's decision.

4.81 ANZ submitted:

> For a licensed credit provider, a complaint under section 23A is likely to also be a complaint for the purposes of RG 165. It will be difficult for licensed credit providers to comply with both sets of requirements. For example, subsection 23B(5) provides for a maximum timeframe of 30 days for resolution, or longer if the complainant agrees in writing. RG 165.94 provides for a maximum timeframe of 45 days with no possibility of extension.[92]

4.82 ARCA made the following suggestion:

> AS ISO 10002-2006 is widely recognised as best practice for managing consumer complaints, and it is widely applied across sectors and scalable to suit a range of organisations in Australia. ARCA strongly recommends

---

87 *Submission 30*, p. 4. Also see Optus, *Submission 31*, p. 4.

88 This code is registered with the telecommunications industry regulator, the Australian Communications and Media Authority.

89 These regulations are administered by the Australian Securities and Investments Commission (ASIC).

90 AS ISO 10002-2006, *Customer satisfaction – Guidelines for complaints handling in organizations* is an International Standard providing guidance for the design and implementation of an effective and efficient complaints-handling process for all types of commercial and non-commercial activities, including those related to e-commerce.

91 *Submission 30*, p. 4. For similar arguments, see: Abacus-Australian Mutuals, *Submission 25*, p. 3; Australasian Retail Credit Association, *Submission 27*, p. 9.

92 *Submission 29*, p. 9. Also see Australasian Retail Credit Association, *Submission 27*, p. 10.

> aligning the timeframes in the Bill with existing obligations for complaints handling and sees no tangible benefit for the misalignment.[93]

4.83 More generally, a few submitters suggested ways in which the existing industry regulations could be accommodated within the Bill. The Australian Finance Conference, for example, recommended:

> …an approach in the provisions dealing with complaint handling that provides an option of alternate compliance to the procedure outlined in the Bill, to compliance with an equivalent standard recognised by the Information Commissioner. This would then facilitate a seamless compliance process for consumer credit providers that, as part of their licensing obligations, were required to implement complaint-handling processes set down by ASIC (eg in its Regulatory Guide 165). A similar approach could also be adopted for broader participants in the industry that are credit providers for the purposes of Part IIIA including the telecommunications industry.[94]

4.84 The Privacy Foundation and the Communications Alliance called for further consideration of the status of existing complaints-handling regulatory regimes under the Bill,[95] with the Communications Alliance making the following suggestion:

> [T]he complaint handling obligations for credit providers [should] be removed from the Bill and instead be dealt with via the industry Credit Reporting Code which is to be developed, to allow different industries to manage such complaints within their existing regulatory frameworks.[96]

4.85 Optus, and others, remarked also on the creation of dual complaint-handling processes:

> Whilst we support the consistency of approach that the Bill is attempting to achieve, its unintended consequence is the creation of inconsistencies in other areas. For all regulated industries, this will institute dual complaint handling processes – one to be followed for credit complaints and another process for all other types of complaints. Given the telecommunications industry already has comprehensive and detailed complaint handling requirements…imposing new and different obligations just for credit complaints will create an administrative burden for telecommunications providers, and confusion for telecommunications customers, who should be

---

93 *Submission 27*, p. 10.

94 *Submission 36*, p. 9. For similar recommendations, see Abacus-Australian Mutuals, which described the Australian Securities and Investments Commission administered complaints-handling regime as 'rigorous and highly prescriptive': *Submission 25*, p. 3.

95 *Submission 49*, p. 34 and *Submission 30*, p. 4, respectively.

96 *Submission 30*, pp 6-7. Also see Optus, *Submission 31*, pp 5-7, for a similar suggestion and identification of the benefits that this would produce.

> able to have a consistent experience with their telecommunications provider regardless of the nature of their complaint.[97]

Departmental response

4.86 The Department advised the committee that it is the government's position that there should be 'a single corrections and complaints process for personal information in the credit reporting system, rather than different processes depending on the industry'.[98] In answer to a question on notice, the Department emphasised the targeted scope and application of the proposed regulatory regime:

> It is only when [a] correction request relates to personal information in the credit reporting system that the corrections request procedures in the Bill would apply. Similarly, the complaint provisions set out in Division 5 of Part IIIA in the Bill only apply where [a] complaint relates to an act or practice that breaches the Privacy Act.[99]

4.87 The Department acknowledged that industry codes may also deal with other credit-related matters – for example, notification processes for consumer credit defaults or serious credit infringements. In such circumstances:

> The Government has imposed specific obligations in relation to these matters and expects that industry codes would be consistent with these obligations.[100]

Commencement of the credit reporting provisions

4.88 Schedule 2 of the Bill will commence nine months after receiving Royal Assent.[101] Some stakeholders did not regard nine months as sufficient lead time for industry to implement the necessary changes.

4.89 A few submitters noted that passage of the Bill is only the first step in a lengthy process to reform the legislative framework for privacy laws in Australia.[102] These submitters contended that the regulations and the industry-developed credit

---

97 *Submission 31*, p. 5. Also see Communications Alliance, *Submission 30*, p. 6; Telstra, *Submission 52*, p. 2.

98 Answer to question on notice, received 14 September 2012, p. 1. The Attorney-General's Department also noted that the issue of inconsistent regulatory regimes was examined by the Senate Finance and Public Administration Legislation Committee in 2010-2011: see Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, pp 78-81.

99 Answer to question on notice, received 14 September 2012, p. 2.

100 Answer to question on notice, received 14 September 2012, p. 2.

101 Item 2 of the table to sub-clause 2(1) of the Bill.

102 For example, see Australian Finance Conference, *Submission 36*, p. 3; Consumer Credit Legal Centre (NSW), *Submission 51*, p. 3.

reporting code will need to be finalised before stakeholders can commit resources to implementation.[103] ARCA, for example, submitted:

> While some organisations are well advanced in their preparation to these reforms, others have noted that they have been unable to design and build the solutions, as they have not known the final shape of the reforms and the impact on their business. Limited available skills, combined with complex business processes, and highly regulated and defined scheduled opportunities to make institution-wide technology changes means that many ARCA Members may find it extremely difficult to implement the required system, training, documentation, and process changes in the proposed timeframe.
>
> The reality of the process attached to the reforms to credit reporting means that there is very little time available for industry to see the final legislative and regulatory detail before the regime is due to start. Given that credit reporting is an integral part of the way more than $1.1 trillion dollars of consumer credit is granted and managed in Australia, it is critical that adequate time be provided to undertake this reform in a controlled and structured manner.[104]

4.90 Abacus-Australian Mutuals (AAM), the Australian Bankers' Association (ABA) and the Australian Finance Conference (AFC) suggested timeframes that, in their view, would be adequate lead time for industry:

- AAM submitted that the commencement date should be 'at least 12 months' from registration of the credit reporting code;[105]
- the ABA proposed 15 to 18 months from the date of Royal Assent;[106] and
- the AFC considered that a reasonable implementation period would be 12 to 18 months after the detail of the reforms has been settled.[107]

4.91 However, the AFC submitted:

> Rather than adopt a fixed date or date tied to date of assent, the AFC recommends an approach that enables a commencement date to be determined by the Minister (akin to the process adopted for the Personal Property Securities Reform) may be the best means of balancing the

103 For example, see ANZ Banking Group Limited, *Submission 24*, p. 3; Australasian Retail Credit Association, *Submission 27*, p. 8; Abacus-Australian Mutuals, *Submission 25*, pp 3-4.

104 *Submission 27*, p. 8.

105 *Submission 25*, p. 5.

106 Mr Steven Münchenberg, Australian Bankers' Association, *Committee Hansard*, 10 August 2012, p. 17.

107 *Submission 36*, p. 4.

> imperatives for early enactment against inadequate lead-times for implementation.[108]

4.92 ARCA considered that the various components of the reform should commence at the same time and proposed a four-step commencement process, which, it argued, would provide certainty and a practical amount of time to finalise the reform and adequately prepare for compliance. ARCA's suggested process was:

- establish a set time once the Bill and regulations have been finalised for the credit reporting code to be developed;
- require the Commissioner to either approve the credit reporting code or make a determination that the Commissioner will draft the credit reporting code within a specified time period;
- if the Commissioner is to draft the credit reporting code, set a time period for such drafting; and
- from the point at which there is a registered credit reporting code set a commencement date for the new privacy regime.[109]

4.93 ARCA anticipated that the regulations would be finalised 'in early 2013 at the earliest' and that the industry-developed credit reporting code (which cannot be completed until after finalisation of the Bill and the regulations) would be presented to the regulator in mid-2013.[110] Officers from the Department confirmed to the committee that draft regulations were released for public comment on 17 August 2012, with submissions due to close on 28 September 2012.[111]

4.94 The CCLCNSW recommended that the Bill should not be passed until the regulations and the credit reporting code have been drafted and considered:

> [R]eviewing just one part of the regulatory framework will mean that it is inevitable there will be matters not covered due to oversight or an expectation that the matter will be covered in another part of the regulation. A particular risk is an expectation that a range of matters will be covered by the Credit Reporting Code of Conduct when this may not be appropriate or even reasonable.[112]

---

108 *Submission 36*, p. 4. For similar comments, see Mr Steven Münchenberg, Australian Bankers' Association, *Committee Hansard*, 10 August 2012, p. 16; Dr David Grafton, Veda, *Committee Hansard*, 10 August 2012, p. 24.

109 *Submission 27*, p. 9.

110 *Submission 27*, p. 9.

111 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 16. Also see Attorney-General's Department, *Proposed regulations under the Privacy Amendment (Enhancing Privacy Protection) Bill: A discussion paper to provide an overview of the relevant regulation making powers under the Bill and the existing Privacy Act 1988, and outline the Government's proposed regulation*, August 2012.

112 *Submission 51*, pp 3-4. For similar comments regarding the need to consider the entire framework, see Australian Privacy Foundation, *Submission 49*, p. 25.

Departmental response

4.95 The Department informed the committee that the standard three-month period between Royal Assent and commencement of the Bill was previously extended (to the current nine-month commencement date) in line with advice received from the OAIC, and to allow sufficient time to register the credit reporting code. In addition:

> [T]he commencement period should provide…certainty by setting out a defined time in the legislation for commencement, and should see all elements of the Privacy Amendment Bill commence at the same time (that is, no staged implementation).[113]

4.96 Further:

> The Department does not consider that commencement should be at the discretion of the Attorney-General, nor does the Department consider that commencement should be contingent on the registration of the [credit reporting] Code as this does not ensure certainty. The Department will be considering stakeholder views on extending the current proposed [nine] month commencement period in proposing options for the Attorney-General's consideration.[114]

113 Additional information, received 29 August 2012, p. 11.

114 Additional information, received 29 August 2012, p. 11.

CHAPTER 5

Australian Information Commissioner's functions and powers

5.1 Under subsection 12(1) of the *Australian Information Commissioner Act 2010* (AIC Act), the 'privacy functions' of the Australian Information Commissioner (Commissioner) are conferred upon the Australian Privacy Commissioner, a person appointed under section 14 of the AIC Act.

Enhanced powers

5.2 Schedule 4 of the Bill makes several amendments to the functions and powers of the Commissioner. The Explanatory Memorandum (EM) indicates that these amendments are largely derived from recommendations made by the Australian Law Reform Commission (ALRC) and are intended to:

> …improve the Commissioner's ability to resolve complaints, recognise and encourage the use of external dispute resolution services, conduct investigations and promote compliance with privacy obligations.[1]

Support for enhanced powers and commensurate resourcing

5.3 Some submitters and witnesses expressed broad support for the Bill's proposed enhancement of the Commissioner's powers.[2] The Australian Privacy Commissioner, Mr Timothy Pilgrim, told the committee:

> These powers reflect the increasing importance that the community places on the protection of personal information and the need for the protection of privacy interests in a digital and globalised world. They will assist me in addressing serious and systemic interferences with the privacy of individuals and provide a clear message to entities of the need to take privacy seriously.[3]

5.4 The NSW Privacy Commissioner submitted similarly:

> [These powers] will hopefully lead to better outcomes for the community in terms of ensuring that entities consider the privacy-related consequences of projects as soon as possible to avoid potential privacy breaches later in the process.[4]

---

1 Explanatory Memorandum (EM), p. 216. Also see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Recommendations 47 and 49-50.

2 For example, Office of the Victorian Privacy Commissioner, *Submission 17*, p. 1; Australian Privacy Foundation, *Submission 49*, p. 4.

3 *Committee Hansard*, 10 August 2012, p. 8.

4 *Submission 42*, p. 10.

5.5 In some instances, submitters referred to specific provisions which they supported. For example, the NSW Privacy Commissioner and the Australian Privacy Foundation (Privacy Foundation) endorsed the proposal to allow the Commissioner to accept enforceable undertakings (proposed new section 33E of the Privacy Act in item 64 of Schedule 4).[5] The Office of the Victorian Privacy Commissioner especially welcomed proposed new section 33D of the Privacy Act, which enables the Commissioner to direct a Commonwealth agency to conduct a 'privacy impact assessment' (PIA):

> It is my hope that these powers are exercised widely, as my office has found that conducting a PIA early in a project has the ability to greatly reduce the impacts on the privacy of individuals…I recommend removing section 33D(7) and allowing the Commissioner to direct any APP entity to conduct a PIA.[6]

5.6 Proposed new subsection 33D(7) of the Privacy Act requires the Attorney-General to undertake a review of proposed new section 33D within five years of its commencement to determine whether the section should apply in relation to private sector organisations, as well as Commonwealth agencies.

5.7 The EM notes that proposed new subsection 33D(7) of the Privacy Act partially implements the Australian Government's response to ALRC Recommendation 47-5.[7] That response states:

> 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 [Recommendation] 47-4 for agencies should not be available in relation to organisations at this stage.[8]

5.8 A few submitters and witnesses also commented on the adequacy of resourcing for the Office of the Australian Information Commissioner (OAIC).[9] Australian Direct Marketing Association (ADMA), for example, submitted that

---

5 *Submission 42*, p. 10 and *Submission 49*, p. 6, respectively. The Australian Privacy Foundation further argued that the Australian Information Commissioner should be required to publish such undertakings: *Submission 49*, p. 6.

6 *Submission 17*, p. 13. The Australian Privacy Foundation suggested that, where a 'privacy impact assessment' is requested by the Australian Information Commissioner, it should be completed before decisions are made to proceed with the activity or function in question: see *Submission 49*, p. 6.

7 EM, p. 233. Also see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 58 (Recommendation 47-5).

8 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, pp 86-87.

9 For example, see Centre for Internet Safety, *Submission 22*, p. 4; Ms Katie Miller, Law Institute of Victoria, *Committee Hansard*, 10 August 2012, p. 47.

under-resourcing of the OAIC, in general, and the Australian Privacy Commissioner, in particular, was a problem when the National Privacy Principles were first introduced in 2001. ADMA's submission argued that this led to delays in the resolution of complaints, which undermined confidence in the effectiveness of the (then) new privacy regime. Accordingly:

> It is to be hoped that the Government will increase the budget for the [Office of the Australian Information Commissioner] commensurate with the new powers and functions contained in [the current proposed] legislation.[10]

Concerns regarding exercise of the powers

5.9 Some submitters and witnesses argued, however, that the Commissioner has not fully utilised the enforcement powers currently available under the Privacy Act.[11] Most notably, the Privacy Foundation submitted:

> [W]e consider that successive Commissioners have had a history of inaction in the use of the enforcement powers that they do have, which has seriously undermined the effectiveness of the Privacy Act...This regrettable situation cannot be reversed solely by more powers or more resources being given to the Commissioner. More powers must also be given to complainants so that they can ensure for themselves that the Commissioner does his or her job.[12]

5.10 In particular, the Privacy Foundation referred to proposed new paragraph 96(1)(c) of the Privacy Act.[13] This provision will allow for an appeal to be made to the Administrative Appeals Tribunal against a decision made by the Commissioner under current subsections 52(1) or 52(1A) (Determination of the Commissioner) of the Privacy Act.[14]

5.11 The Privacy Foundation described this provision as a 'long-overdue reform'[15] but remained sceptical of its value given the low number of determinations made under section 52 of the Privacy Act to date:

> [F]or the right of appeal to have any meaning, the Commissioner would first have to make decisions against which appeals can be lodged.

---

10 *Submission 7*, p. 9.

11 For example, see Ms Katherine Lane, Consumer Credit Legal Centre (NSW), *Committee Hansard*, 10 August 2012, p. 29; Australian Privacy Foundation, *Submission 49*, p. 4.

12 *Submission 49*, p. 4.

13 Item 200 of Schedule 4 of the Bill.

14 Subsection 52(1) of the Privacy Act provides that, after investigating a complaint, the Commissioner may make a determination dismissing the complaint or find the complaint substantiated and make a determination. Subsection 52(1A) of the Privacy Act extends the meaning of 'loss or damage' in subsection 52(1) to include injury to the complainant's feelings or humiliation suffered by the complainant.

15 *Submission 49*, p. 4.

> In the 23 year history of the Privacy Act, successive Commissioners have made a mere nine determinations. It is a very poor record of inaction.
>
> Therefore, this new right of appeal is of little use unless complainants can require the Commissioner to make formal decisions under s52 of the Act…The only way to make the new s96 right of appeal meaningful is therefore for the Commissioner to be required to make a formal decision dismissing a complaint, whenever a complainant so requests, so as to activate a complainant's right of appeal.[16]

5.12 In response, the Australian Privacy Commissioner, Mr Pilgrim, advised the committee that the low number of determinations reflects success in conciliating matters rather than having to use more formal powers. Further:

> [W]e have a system that is set up to bring the parties together in an area that is not based around black-and-white law. It is an area where there are a lot of judgment calls to be made on broad-ranging principles and the process that we take to resolve the complaints reflects the nature of the [A]ct in that regard.[17]

5.13 Mr Pilgrim rejected the suggestion that individuals should have the ability to require the Commissioner to make a determination,[18] a position also taken by the Australian Government when it rejected a similar recommendation made by the ALRC in 2008:

> 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.[19]

5.14 Mr Pilgrim noted that a decision not to go to determination is appellable under section 5 of the *Administrative Decisions (Judicial Review) Act 1977*, and argued that it would be quite reasonable for this right to extend to a merits-based review of any determination made by the Commissioner.[20]

---

16 *Submission 49*, p. 4. The Australian Privacy Foundation added that the Australian Information Commissioner should be required to make the determination within 60 days: see *Supplementary Submission 49*, p. 1.

17 *Committee Hansard*, 10 August 2012, p. 11.

18 *Committee Hansard*, 10 August 2012, p. 11.

19 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, p. 93. Also see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC 108), May 2008, p. 59 (Recommendation 49-5).

20 *Committee Hansard*, 10 August 2012, p. 11. Also see Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC 108), May 2008, p. 60 (Recommendation 49-7).

5.15 Mr Pilgrim's comments regarding the number of determinations to date were endorsed by the Department:

> The Department is not aware of any evidence of widespread dissatisfaction with the way in which the Commissioner has resolved complaints through the conciliation process.[21]

5.16 The Department did not agree, however, that there should be a right to merits-based review of the Commissioner's decision not to make a determination:

> [E]xpanding merits review to decisions by the Commissioner not to make a determination, or including a right of complainants to require the Commissioner to make a determination, would be at odds with the compliance-oriented regulatory design recommended by the ALRC [and adopted throughout Schedule 4 of the Bill].[22]

Civil penalty orders

5.17 Schedule 4 of the Bill also inserts a new Part VIB into the Privacy Act.[23] Proposed new Part VIB sets out provisions in relation to civil penalty orders. Essentially, an entity will be prohibited from contravening a 'civil penalty provision',[24] and the new Part provides a means by which the Commissioner can enforce these provisions.

5.18 Proposed new section 80W of the Privacy Act allows the Commissioner to apply to the Federal Court of Australia or the Federal Magistrates Court for an order that an entity, which is alleged to have contravened a 'civil penalty provision', pay the Commonwealth a pecuniary penalty.[25] The court may, if satisfied that an entity has contravened a 'civil penalty provision', order the entity to pay the Commonwealth such pecuniary penalty as the court deems to be appropriate. The maximum penalty that the court can order is:

> (a) if the entity is a body corporate—5 times the amount of the pecuniary penalty specified for the civil penalty provision; or
>
> (b) otherwise—the amount of the pecuniary penalty specified for the civil penalty provision.[26]

---

21 Additional information, received 29 August 2012, p. 11.

22 Additional information, received 29 August 2012, pp 12-13.

23 Item 189 of Schedule 4 of the Bill.

24 Proposed new section 80V of the Privacy Act; item 189 of Schedule 4 of the Bill. A 'civil penalty provision' will be a section or subsection of the Privacy Act which contains the words 'civil penalty' and sets out a civil penalty amount: see proposed new section 80U of the Privacy Act; item 189 of Schedule 4 of the Bill.

25 Item 189 of Schedule 4 of the Bill.

26 Proposed new subsection 80W(3) of the Privacy Act; item 189 of Schedule 4 of the Bill. Also see proposed new section 80Z (item 189 of Schedule 4 of the Bill), which will allow the court to make a single penalty order for certain multiple contraventions of a 'civil penalty provision'; and Facebook, Google, IAB Australia and Yahoo!7, which called for clarification of the application of the 'totality' principle: *Submission 39*, p. 9.

Clarity and proportionality

5.19 Some submitters commented on the judicial discretion in proposed new subsection 80W(3) of the Privacy Act. ADMA, for example, expressed concern that the court could theoretically impose unlimited fines because the wording of the penalty provisions is 'too open-ended'.[27] Several other submitters similarly called for clarification of the proposed fines and penalties provisions.[28]

5.20 Magnamail, and others, argued:

> Being a company that is subject to the Privacy Act it is essential that we have an understanding of the potential extent of fines and penalties for our risk assessment purposes.[29]

5.21 Remington Direct added:

> Despite the Government's best efforts to educate, there are likely to be companies who don't read the literature or realise it applies to them. In light of this we would support an initial warning before a company incurs a monetary fine.[30]

5.22 A few submitters also questioned the penalties contained in certain 'civil penalty provisions'. The Law Council of Australia, for example, argued in a general sense that a number of large penalties contained in the Bill are 'out of proportion to the gravity of the contraventions involved'.[31] More specifically, the Australian Industry Group considered that proposed new section 13G of the Privacy Act should provide for an 'appropriate' civil penalty of 60 units, rather than the 'excessive' 2,000 units included in the provision.[32]

---

27 *Submission 7*, p. 8.

28 For example, GEON, *Submission 37*, p. 2; Facebook, Google, IAB Australia and Yahoo!7, *Submission 39*, p. 9.

29 *Submission 9*, p. 3. Identical statements were made by Remington Direct, *Submission 10*, p. 2; Pareto Phone and Pareto Fundraising, *Submission 11*, p. 3; The Mailing House, *Submission 15*, p. 4; Acxiom Australia, *Submission 32*, p. 3; Kimberly Clark Australia, *Submission 46*, p. 3; Greater Data, *Submission 58*, p. 3.

30 *Submission 10*, p. 2.

31 *Submission 14*, p. 12. By way of example, the Law Council of Australia's submission contrasted proposed new section 20P of the Privacy Act (a 'civil penalty provision' with a penalty of 2,000 units) with current section 18G of the Privacy Act, which provides that a credit reporting agency in possession or control of certain information must take reasonable steps to ensure that personal information is accurate, up-to-date, complete and not misleading. Section 18G of the Privacy Act is not a civil penalty provision.

32 *Submission 16*, p. 3. Proposed new section 13G of the Privacy Act makes serious and repeated interferences by an entity with the privacy of an individual a civil offence: see item 50 of Schedule 4 of the Bill. Also see Australian Bankers' Association, *Submission 24*, p. 14 for similar comments.

5.23 The NSW Privacy Commissioner, who supported proposed new section 13G of the Privacy Act, did not agree that the penalty in that provision is disproportionate:

> The community expects that there will be appropriate penalties for organisations that engage in serious and repeated acts that interfere with the privacy of an individual or individuals.[33]

5.24 A representative from the Department agreed:

> [There] is potentially a high penalty, only for serious or repeated interferences with privacy. If you think of the regulatory scheme at the pyramid, it is at the apex of the pyramid. It says, 'This is the ultimate sanction that a commissioner could take.' It is designed to be used only in those situations where there are really serious issues that have emerged or there is a repeated pattern of behaviour that has not otherwise been resolved through the other tools that the commissioner has available to him.[34]

5.25 The Australasian Retail Credit Association (ARCA) and ADMA, in respect of proposed new section 13G of the Privacy Act, argued that the Bill should allow for breaches which are not wilful or deliberate. ARCA suggested that, as with the *Corporations Act 2001*, 'lesser penalties' should be applied in such circumstances; and ADMA recommended that section 13G of the Privacy Act should be amended to define 'serious' as 'reckless or wilful and intentional'.[35]

5.26 The EM acknowledges that proposed new section 13G of the Privacy Act does not define what constitutes a 'serious' or 'repeated' interference with the privacy of an individual – that is, the ordinary meaning of these words will apply.[36] In addition:

> [I]t is anticipated that the OAIC will develop enforcement guidelines which will set out the criteria on which a decision to pursue a civil penalty will be made. These guidelines will assist in [providing] further clarity and context for the term ['serious'].[37]

5.27 In its submission, the Australian Bankers' Association (ABA) noted that the Bill does not provide any defence to an alleged interference with the privacy of an individual. In the ABA's view, 'there should be a general defence available to an APP entity' for inadvertent breaches of the Privacy Act:

> The amendments in the Bill will create a more onerous compliance regime for APP entities in the collection, handling, use and disclosure of personal information.
>
> Banking is a highly dynamic environment for the handling of personal information across a very large number of employees. Banks will continue

---

33 *Submission 42*, p. 10.

34 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 4.

35 *Submission 27*, p. 18 and *Submission 7*, p. 8, respectively.

36 EM, p. 226.

37 EM, p. 227.

> to develop and implement robust privacy protection systems and processes and will rigorously train staff as they have done to date.
>
> Inadvertent breaches of the [Privacy] Act and the APPs may occur in circumstances where these occurrences ought fairly to be excused.[38]

38 *Submission 24*, p. 15.

CHAPTER 6

Committee views and recommendations

6.1 This inquiry was one of several reviews into Australia's privacy legislation which have taken place over the past seven years. In particular, the committee notes the extensive review conducted by the Australian Law Reform Commission (ALRC), which reported in August 2008, and to which the Australian Government partially responded in October 2009.

6.2 The Bill gives effect to that response, and the committee understands that a further response will be considered in separate legislation after the Bill's passage and implementation. The second stage response will relate primarily to health services and research provisions, as well as the ALRC recommendations not addressed in the government's first stage response.[1]

6.3 According to the Attorney-General, the Bill aims to bring Australia's privacy protection framework into the modern era.[2] The committee commends such a reform, noting that Australia's privacy laws have not kept pace with the considerable social changes that have occurred since the Privacy Act was first enacted over 20 years ago.[3]

6.4 The reforms introduced in the Bill cover 197 of the 295 policy recommendations made by the ALRC and focus on four key objectives.[4] In this report, the committee has focussed on three key areas:

- the creation of the Australian Privacy Principles (APPs);
- the introduction of more comprehensive credit reporting; and
- the proposed clarification and enhancement of the functions and powers of the Australian Information Commissioner (Commissioner).

6.5 The committee notes that many issues in relation to these proposed amendments have previously been considered by both the ALRC and the Senate Finance and Public Administration Legislation Committee (F&PA committee)

---

1 See http://www.ag.gov.au/Privacy/Pages/Privacy-Reforms.aspx (accessed 31 August 2012); Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 2.

2 The Hon. Nicola Roxon MP, Attorney-General, *House of Representatives Hansard*, 23 May 2012, p. 5211.

3 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, p. 5.

4 Explanatory Memorandum (EM), p. 1. Also see Australian Law Reform Commission, *For Your Information, Australian privacy Law and Practice*, ALRC 108, May 2008, pp 25-102.

in its comprehensive examination of Exposure Drafts of the Bill in 2010-2011.[5] The committee acknowledges that certain issues continue to concern stakeholders but, in instances where the Australian Government has made and communicated clear policy decisions, the committee will not be revisiting those concerns in recommendations in this report.

Australian Privacy Principles

6.6 The creation of the APPs represents an important milestone in the reform of Australia's privacy laws. The committee welcomes the creation of a single set of privacy principles applicable to both Commonwealth agencies and private sector organisations (item 82 of Schedule 1 of the Bill).

6.7 Throughout the inquiry, stakeholders commented on both the APPs and their supporting provisions in Schedule 1 of the Bill. Based on the evidence received, the committee considers that individual privacy protections could be enhanced with some further legislative amendments in relation to key definitions and specific aspects of APP 2, APP 7 and APP 8.

Complexity of the APPs

6.8 The committee notes that, in 2011, the F&PA committee recommended that the draft APPs should be reconsidered with a view to improving their clarity and avoiding repetition.[6] In the current inquiry, the Attorney-General's Department (Department) confirmed that the APPs have been restructured to reduce length and repetition, particularly through the use of a table in proposed new section 16A (item 82 of Schedule 1).[7]

6.9 The committee notes that there remain concerns regarding the complexity of the APPs[8] but accepts the Department's view that ALRC Recommendation 5-2, which called for the Privacy Act to be redrafted to achieve greater logical consistency, simplicity and clarity, has been implemented effectively.[9] The Department advised the

---

5 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/report_part1/index.htm (accessed 2 August 2012);

Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, available at: http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/report_part2/index.htm (accessed 2 August 2012).

6 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 18 (Recommendation 1).

7 Additional information, received 3 September 2012, p. 1.

8 For example, Law Council of Australia, *Submission 14*, p. 8.

9 Additional information, received 29 August 2012, p. 1; answer to question on notice, received 3 September 2012, p. 13.

committee that it considers that the drafting style adopted in the Bill reflects current best drafting practice.[10]

6.10 Nonetheless, the committee considers that the introduction of the APPs must be complemented by educational resources and guidance material for individuals, government agencies and private sector organisations. A number of targeted recommendations in relation to education and guidance on specific APPs were made by the F&PA committee during the course of its inquiry, and those recommendations were endorsed by the Australian Government. However, the need for public awareness and education campaigns on the APPs generally, as well as APP-related guidance material for agencies and organisations, does not appear to have been considered in the F&PA committee's recommendations.

Australian Privacy Principle 2

6.11 The committee supports the introduction of APP 2, which gives an individual the right not to identify him or herself, or to use a pseudonym, when dealing with an APP entity in relation to a particular matter. The committee notes that this right is not absolute, including where it is 'impracticable' for an APP entity to deal with individuals who have not identified themselves (APP 2.2(b)).

6.12 Facebook, Google, IAB and Yahoo!7 suggested that the EM to the Bill should provide examples of impracticability, and that APP 2.2(b) should be extended to include individuals who have used a pseudonym.[11] The committee notes that the Australian Government is 'considering options to enhance clarity around the application of this exception'.[12] In that circumstance, the committee suggests that the government give consideration to amending APP 2.2(b) to refer to 'individuals who have not identified themselves or who have used a pseudonym'.

Recommendation 1

6.13 The committee recommends that the application of the exception in proposed APP 2.2(b) be clarified to make it clear that APP 2.1 does not apply where it is impracticable for the APP entity to deal with 'individuals who have not identified themselves or who have used a pseudonym'.

Australian Privacy Principle 3

6.14 APP 3 prohibits an APP entity from collecting personal information (other than sensitive information) unless the information is 'reasonably necessary' for one or more of the entity's functions or activities. In the case of an agency, the information can also be 'directly related to' one or more of the entity's functions or activities.

6.15 The committee acknowledges the concerns of some stakeholders regarding the breadth of APP 3, and notes that the two components which are the cause of concern are the terms 'reasonably necessary' and 'directly related to'.

---

10 Answer to question on notice, received 3 September 2012, p. 13.

11 *Submission 39*, pp 2-3.

12 Answer to question on notice, received 3 September 2012, p. 4.

6.16 In response to the F&PA committee's 2010-2011 inquiry, the Australian Government stated its support for the use of the 'reasonably necessary' test in APP 3 on the grounds that this objective element 'is intended to reduce instances of inappropriate collection of personal information'.[13] The Department confirmed this policy position in evidence to the current inquiry.[14]

6.17 In relation to the 'directly related to' test in APP 3, the Australian Government accepted the F&PA committee's recommendation to limit this test to Commonwealth agencies only.[15] Submitters – such as the Law Council of Australia and the NSW Privacy Commissioner – argued that all APP entities, including private sector organisations, should be subject to the same obligations regarding the collection of personal information,[16] and that the 'directly related to' test for Commonwealth agencies should be removed from the Bill.

6.18 The government has previously considered the application of the 'directly related to' test. The committee accepts the Department's position that this test imports a defined element for Commonwealth agencies which are required to collect personal information to effectively carry out specific functions and activities, but which might not meet an objective 'reasonably necessary' test. In this context, Commonwealth agencies are also subject to stricter oversight and accountability mechanisms through the parliament, the executive and the Commonwealth Ombudsman.[17]

6.19 The committee also received evidence from some stakeholders regarding the current definition of 'consent' in subsection 6(1) of the Privacy Act and its application to APP 3.3. In 2008, the ALRC considered that the application of this term to the privacy principles should be guided by the Commissioner.[18] The Australian Government accepted this recommendation[19] and, in 2011, the F&PA

---

13 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 3.

14 Additional information, received 29 August 2012, p. 3.

15 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 72 (Recommendation 8); Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 3.

16 *Submission 14*, p. 6 and *Submission 42*, p. 5, respectively.

17 Answer to question on notice, received 3 September 2012, p. 5.

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Volume 1, p. 686 (Recommendation 19-1).

19 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, p. 38.

committee supported its expeditious implementation.[20] The committee considers that the matter now rests with the Commissioner but notes that, in some instances, there may be strong arguments in favour of specific requirements for express consent – for example, in the collection of 'sensitive information'.[21]

Australian Privacy Principle 5

6.20 The committee supports the inclusion of a notification requirement in the APPs in relation to the collection of personal information. As noted by the Office of the Victorian Privacy Commissioner, APP 5 promotes transparency and ensures individuals are aware of their rights in relation to the collection of personal information by an APP entity.[22]

6.21 The committee notes stakeholders' concerns regarding the practical operation of the notification requirement in APP 5.1, and considers that the educational resources and guidance material to be developed and published by the Commissioner should help to address these concerns. In this context, the committee also observes that implementation issues are a particular matter for the APP codes and credit reporting codes to be developed in accordance with Schedule 3 of the Bill at a later time.

Australian Privacy Principle 6

6.22 APP 6 deals with the use or disclosure of personal information. The OAIC did not consider APP 6.3 to be a necessary provision.[23] APP 6.3 allows non-law enforcement agencies to disclose biometric information or biometric templates to 'enforcement bodies', subject to rules made by the Commissioner.

6.23 The Department advised the committee:

> The policy intention of APP 6.3 is to enable non-law enforcement agencies to disclose biometric information and templates for a secondary purpose to enforcement bodies where an APP 6 exception, including the enforcement related activity exception, is not applicable. This may occur where the disclosure is for purposes such as identity/nationality verification or general traveller risk assessment, in circumstances where there is a legitimate basis for the disclosure but no criminal enforcement action is on foot…The policy rationale in APP 6.3 recognises that non-law enforcement agencies have current, and will have future, legitimate reasons to disclose biometric information and templates to enforcement bodies, but that this should occur within a framework that protects against improper disclosure.[24]

---

20 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 33 (Recommendation 4).

21 NSW Privacy Commissioner, *Submission 42*, p. 6.

22 *Submission 17*, p. 7.

23 *Submission 47*, p. 19.

24 Answer to question on notice, received 3 September 2012, pp 7-8.

6.24 The committee accepts this position. In particular, the committee notes that the disclosure will be subject to oversight by the Commissioner and additional safeguards throughout the Privacy Act (due to the classification of biometric information and biometric templates as 'sensitive information').[25] The committee considers that these safeguards will curb any potential abuse of the provision.

Australian Privacy Principle 7

6.25 The committee notes that APP 7, dealing with direct marketing, has been significantly revised to improve its structure and clarity following a recommendation from the F&PA committee.[26] The committee agrees that the provision is much improved, and is consistent with the drafting style used in respect of other APPs which prohibit and then allow certain activities. The committee understands that this is a common approach:

> [C]asting the principle as a 'prohibition' against certain activity followed by exceptions is a drafting approach used in principles-based privacy regulation to clearly identify the information-handling activity that breaches privacy, followed by any exceptions to this general rule that would permit an entity to undertake the activity.[27]

6.26 The committee accepts this rationale, but acknowledges the concerns raised by the Australian Direct Marketing Association, and others, regarding the heading to APP 7.1 ('Prohibition on direct marketing').[28] The committee does not perceive any particular justification for this heading, which is unique among the APPs. The committee agrees with stakeholders that it is likely to cause considerable confusion.

Recommendation 2

6.27 The committee recommends that, to avoid confusion, the subheading to proposed APP 7.1 in item 104 of Schedule 1 of the Bill be amended to read 'Use or disclosure' or 'Direct marketing', rather than 'Prohibition on direct marketing'.

6.28 In 2010-2011, the F&PA committee recommended that consideration be given to restructuring the exceptions to the general prohibition on direct marketing contained in APP 7.1.[29] The committee notes that these provisions – APP 7.2 and

---

25 Answer to question on notice, received 3 September 2012, p. 7.

26 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 142 (Recommendation 10); Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles*, May 2012, p. 8.

27 Attorney-General's Department, additional information, received 29 August 2012, p. 1.

28 *Submission 7*, p. 2.

29 Senate Finance and Public Administration Legislation Committee, *Exposure Drafts of Australian Privacy Amendment Legislation, Part 1 – Australian Privacy Principles*, June 2011, p. 150 (Recommendation 13).

APP 7.3 – have not been substantively amended. In the current inquiry, the issue of most concern to stakeholders was the opt-out notification requirement in APP 7.3(d).

6.29 The committee heard stakeholders' concerns regarding the clarity and implementation of the requirement, particularly in relation to social media technologies. However, the committee is persuaded that the requirement is flexible and feasible, while requiring organisations to adapt to new direct marketing rules which enhance the privacy protections of consumers.[30]

6.30 The Australian Privacy Foundation argued that the opt-out mechanisms in APP 7.2 and APP 7.6 could be strengthened with the inclusion of similar notification requirements.[31] The committee notes that the distinction between these two provisions and APP 7.3 is the element of reasonable expectation: APP 7.2 provides for situations where an individual would reasonably expect a private sector organisation to use or disclose personal information for direct marketing purposes (APP 7.2(b)), whereas APP 7.3 applies to situations where there is no such expectation. The committee agrees however that, regardless of expectation, individuals might wish to opt-out of direct marketing communications at any time.

Recommendation 3

6.31 The committee recommends that proposed APP 7.2 and APP 7.6 in item 104 of Schedule 1 of the Bill be amended to ensure consistency with the notification requirement in APP 7.3, and enable individuals the opportunity to opt-out of direct marketing communications at any time.

Australian Privacy Principle 8

6.32 The committee received considerable evidence in relation to the cross-border disclosure of personal information, and recognises that this is a particularly complex legal and policy issue. The complexity arises from the creation of two regimes within the Bill,[32] conflict of laws issues and the competing interests of various stakeholders. In this regard, a balance must be struck between protecting the privacy of individuals and facilitating the free flow of information across national borders.

6.33 In general, most stakeholders supported the intent of APP 8 but expressed concerns regarding the accountability mechanism in proposed new section 16C of the Privacy Act. The committee notes concerns that an APP entity could be held liable for privacy breaches committed by an 'overseas recipient' even though the entity has taken all reasonable steps to prevent that breach.[33]

---

30 Attorney-General's Department, additional information, received 29 August 2012, pp 2-3.

31 *Submission 49,* p. 17.

32 That is, the 'Australian link' provision discussed in the context of credit reporting and APP 8 in conjunction with its accountability mechanism in proposed new section 16C of the Privacy Act.

33 For example, Facebook, Google, IAB Australia and Yahoo!7, *Submission 39,* pp 6-7; Law Council of Australia, *Submission* 14, p. 11; Australian Bankers' Association, *Submission 24,* p. 11.

6.34 In evidence, departmental officers acknowledged the difficulties which could arise in a conflict of laws situation and for which there is no current solution.[34] In relation to inadvertent breaches – caused, for example, by hacking, fraud or an 'overseas recipient's' recklessness or negligence – the Department emphasised the need for privacy protection and for individuals to have a means of redress.[35] The committee accepts this position, noting that the circumstances of each case can be considered by the Commissioner investigating a complaint under Part V of the Privacy Act.

6.35 The committee also notes the Australian Government's stated policy position:

> The exceptions in APP 8.2 have been carefully considered and the Government considers that they are justified. The Government considers that these exceptions provide appropriate and reasonable grounds for the transfer of accountability to an overseas recipient. In all other situations, the Australian entity should continue to remain accountable for the protection of personal information.[36]

6.36 APP 8.2(b) provides an exception to APP 8.1 where an APP entity expressly informs an individual that consent to the disclosure of the information renders APP 8.1 inapplicable, and the individual then gives an informed consent to the cross-border disclosure of their personal information. The OAIC expressed concern regarding the potential 'displacement' of the accountability mechanism,[37] and the committee agrees with the NSW Privacy Commissioner that APP 8.2(b) should better explain the practical effect and potential consequences of this displacement.[38]

Recommendation 4

6.37 The committee recommends that proposed APP 8.2(b) in item 104 of Schedule 1 of the Bill be amended to require an entity to inform an individual of the practical effect and potential consequences of any informed consent by the individual to APP 8.1 not applying to the disclosure of the individual's personal information to an 'overseas recipient'.

Recommendation 5

6.38 The committee recommends that the Explanatory Memorandum to the Bill be revised to clearly explain that an entity will be required to inform an individual of the practical effect and potential consequences of any informed consent by the individual to APP 8.1 not applying to the disclosure of the individual's personal information to an 'overseas recipient'.

---

34 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, pp 5-6.

35 Additional information, received 29 August 2012, p. 13.

36 Additional information, received 29 August 2012, p. 13.

37 *Supplementary Submission 47*, pp 1-2.

38 *Submission 42*, p. 8.

'Enforcement body' and 'enforcement related activity'

6.39 The committee notes that item 17 of Schedule 1 of the Bill, defining the 'Immigration Department' (currently the Department of Immigration and Citizenship) as an 'enforcement body', was a matter of concern for the Office of the Australian Information Commissioner (OAIC) because the Immigration Department's usual activities are 'not of an enforcement related nature'.[39] The committee also notes that this aspect of the definition was not included in the Exposure Draft of the Bill. While the Explanatory Memorandum (EM) contains a brief statement regarding the appropriateness of this provision,[40] the committee considers that further details should be provided to give examples of the types of enforcement-related functions and activities which will be covered by the exception.

6.40 The committee also acknowledges the concerns of Liberty Victoria and the Australian Privacy Foundation regarding the addition of surveillance activities, intelligence-gathering activities and other monitoring activities to the definition of 'enforcement related activity' (item 20 of Schedule 1 of the Bill). The EM justifies this amendment on the basis of accuracy and modernisation:

> These types of activities have been included to update and more accurately reflect the range of activities that law enforcement agencies currently undertake in performing their legitimate and lawful functions of accuracy and modernisation.[41]

6.41 The committee suggests, however, that this explanation should be expanded to provide further guidance on what will constitute lawful use of an individual's personal information by 'enforcement bodies'.

Recommendation 6

6.42 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill to clearly explain the enforcement-related functions and activities of the Department of Immigration and Citizenship, as justification for the classification of the 'Immigration Department' as an 'enforcement body' in item 17 of Schedule 1 of the Bill.

Recommendation 7

6.43 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill to clearly explain the scope and intended application of the terms 'surveillance activities', 'intelligence gathering activities', and 'monitoring activities' in item 20 of Schedule 1 of the Bill.

---

39 *Submission 47*, p. 13.

40 EM, p. 57.

41 EM, p. 58.

'Permitted general situation'

6.44 Some stakeholders commented on proposed new section 16A of the Privacy Act (item 82 of Schedule 1 of the Bill), which consolidates and separates an exception repeated throughout various APPs in the Exposure Drafts of the Bill examined by the F&PA committee. In particular, the Law Council of Australia pointed out that it might be difficult to read and interpret the legislation due to the separation of the exception from its substantive provisions.[42]

6.45 The committee agrees that, in this regard, the legislation could be more 'user-friendly', and considers that a relevant note at the end of each APP should be inserted where necessary. This applies equally to proposed new section 16B of the Privacy Act, which defines the 'permitted health situation' exception.

6.46 One exception contained in the definition of 'permitted general situation' relates to 'diplomatic or consular functions or activities' (item 6 in the table to proposed new subsection 16A(1) of the Privacy Act). The OAIC submitted that the scope of this exception is not clear.[43] The committee agrees that a clear explanation of the meaning of the phrase 'diplomatic and consular functions' would help identify the range of activities which are to be exempted from the application of the APPs.

Recommendation 8

6.47 The committee recommends that the provisions contained in item 82 of Schedule 1 of the Bill and for each Australian Privacy Principle which contains a 'permitted general situation' or 'permitted health situation' exception, a note should be added at the end of the relevant principle to cross-reference proposed new section 16A of the *Privacy Act 1988* and/or proposed new section 16B of the *Privacy Act 1988*, as appropriate.

Recommendation 9

6.48 The committee recommends that the Attorney-General's Department revise and reissue the Explanatory Memorandum to the Bill to explain the intended scope and application of the 'diplomatic or consular functions or activities' exception set out in item 6 in the table to proposed new subsection 16A(1) of the Privacy Act in item 82 of Schedule 1 of the Bill.

Credit reporting definitions

6.49 The committee notes the numerous comments regarding amendments to the general definitions in subsection 6(1) of the Privacy Act and key definitions relating to credit reporting in proposed new Division 2 of Part II (Interpretation) of the Privacy Act (item 69 of Schedule 2 of the Bill). The committee will not comment on each proposed definition but focuses its attention instead on those definitions which appear to be most contentious or significant.

---

42 *Submission 14*, p. 8.

43 *Submission 47*, p. 11.

'Australian link'

6.50 The committee heard that the 'Australian link' requirement in proposed new paragraph 21G(3)(b) of the Privacy Act will significantly affect a number of stakeholders' business operations. Departmental representatives assured the committee that such an effect is not intended and a solution is currently being considered.[44] The committee is therefore confident that this concern will be addressed in due course.

6.51 The Bill proposes two new regimes for the cross-border disclosure of personal information: the 'Australian link' requirement, which is used throughout proposed new Part IIIA of the Privacy Act (credit reporting provisions); and the general obligations set out in APP 8, supported by an accountability mechanism in proposed new section 16C of the Privacy Act (item 82 of Schedule 1 of the Bill).

6.52 In relation to proposed new section 21G, the committee understands that the 'Australian link' requirement creates a special rule for the cross-border disclosure of 'credit eligibility information'[45] and is entirely separate from the APP 8 regime. While some finance and credit industry stakeholders questioned the need for the two regimes, the committee accepts that the Australian Government has carefully considered the structural approach adopted in the Bill.[46]

Key definitions

6.53 The committee appreciates that the proposed key definitions relating to credit reporting are numerous and, in some instances, circuitous. In this regard, the committee notes the stated need for specific terms which correlate with information flows in the credit reporting system, as well as the APPs in Schedule 1 of the Bill.[47] The committee also notes the Commissioner's new guidance-related function (item 54 of Schedule 4 of the Bill), which includes promoting an understanding and acceptance of the credit reporting provisions, and the Australian Government's previous commitment to educate and inform stakeholders in the transition phase of the Bill.[48]

'Default information'

6.54 The committee acknowledges concerns regarding proposed new subsection 6Q(1) of the Privacy Act (item 69 in Schedule 2 of the Bill) (key definition of 'default information'). With respect to notification and listing processes, the committee agrees with the Consumer Credit Legal Centre (NSW) that, after receiving written notification of a default, consumers should have a period of time in which to rectify that default before a listing can be made.

---

44 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 5; Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 2.

45 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 10 August 2012, p. 5.

46 See EM, p. 91.

47 EM, p. 93.

48 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Draft of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 4.

6.55 The Australian Communications Consumer Action Network suggested that a 'credit provider' should be required to notify an individual of the intention to make a default listing. The committee does not consider this notification to be necessary but agrees that consumers should be aware of the potential outcome of a failure to rectify a default.

6.56 The committee agrees with the threshold amount in proposed new subparagraph 6Q(1)(d)(i) (item 69 of Schedule 2) being increased to avoid the capture of relatively small debts as a consumer credit default, particularly those related to telecommunications and utility debts. Noting that a $300 minimum attracted the most support, the committee suggests that the Australian Government actively consider increasing the threshold to at least this amount.

6.57 The committee understands that there are a number of industry views regarding the time in which a listing should be made. The committee agrees that there should be some certainty in the process, particularly to avoid the potentially adverse effects identified by the Energy & Water Ombudsman NSW – for example, considerably delayed default listings.[49] The Australian Government has previously supported clarification on this issue,[50] and the committee endorses the view that appropriate guidance should be provided in the industry-developed credit reporting code.

6.58 The committee agrees with the Financial Ombudsman Service that individuals experiencing financial hardship should not be discouraged from approaching their 'credit provider' in order to negotiate a hardship arrangement under the *National Consumer Credit Protection Act 2009* (National Consumer Credit Protection Act).[51] The committee is concerned to hear that individuals are increasingly being default-listed while negotiating such arrangements, and therefore supports better alignment between the National Consumer Credit Protection Act and the Privacy Act.

Recommendation 10

6.59 The committee recommends that proposed new subsection 6Q(1) in item 69 of Schedule 2 of the Bill be amended to require an appropriate amount of time, such as 14 days, to have elapsed from the date of a written notice before a default listing can occur.

Recommendation 11

6.60 The committee recommends that the written notification in proposed new subsection 6Q(1) in item 69 of Schedule 2 of the Bill be amended to include a warning about the potential for a default listing by a 'credit provider' in the event that an overdue amount is not paid within a set period of time.

---

49 *Submission 38*, p. 4.

50 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Draft of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 9.

51 Answer to question on notice, received 23 August 2012, pp 2-3.

Recommendation 12

6.61 The committee recommends that proposed new subparagraph 6Q(1)(d)(i) in item 69 of Schedule 2 of the Bill be amended to reflect $300, or such higher amount as the Australian Government considers appropriate, as the minimum amount for which a consumer credit default listing can be made.

Recommendation 13

6.62 The committee recommends that the Office of the Australian Information Commissioner, in formulating guidelines under proposed new section 26V in item 72 of Schedule 2 of the Bill, include as a criterion the timeframe within which an individual's 'default information' can be listed by a 'credit provider'.

Recommendation 14

6.63 The committee recommends that the Office of the Australian Information Commissioner, in formulating guidelines under proposed new section 26V in item 72 of Schedule 2 of the Bill, include a requirement for credit providers to fully consider an application for financial difficulty assistance under the *National Consumer Credit Protection Act 2009* before an individual's 'default information' can be listed.

'Serious credit information'

6.64 Submitters and witnesses also raised specific concerns regarding the proposed new definition of 'serious credit infringement' in subsection 6(1) of the Privacy Act (item 63 of Schedule 2 of the Bill).

6.65 The committee recognises the significance and potential consequences of listing a 'serious credit infringement' as part of a consumer's 'credit information'. The committee considers it appropriate for a 'credit provider' to be required to take such steps as are reasonable in the circumstances (proposed new paragraph (c)(ii)) for at least six months (proposed new paragraph (c)(iii)) in an effort to contact a debtor.

6.66 The committee does not accept that the proposed definition of 'serious credit infringement' should be removed from the Bill, as suggested by the Consumer Action Law Centre. Instead, the committee agrees with the view expressed by the Australian Law Reform Commission in its 2008 report that 'credit providers' have a legitimate interest in sharing information about the conduct of individuals that falls short of fraud.[52] The committee endorses the approach adopted in the Bill, an approach which the committee considers does not diminish the serious nature of fraud.

52 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, May 2008, Volume 3, p. 78.

'New arrangement information'

6.67 The committee notes that pre-default hardship arrangements are governed by provisions in the National Consumer Credit Protection Act, whereas post-default hardship arrangements are to be dealt with as 'new arrangement information' under the Privacy Act.

6.68 The committee is concerned to have heard that the non-alignment of these two regimes could operate to the detriment of individuals who are complying with a hardship arrangement. The ANZ Banking Group Limited suggested that the credit reporting system could note this compliance and avoid adversely affecting an individual's credit file and future ability to obtain credit.[53] However, the committee received evidence from Ms Katherine Lane of the Consumer Credit Legal Centre (NSW) that any such notation could discourage consumers from requesting hardship variations under section 72 of the National Consumer Credit Protection Act.[54]

6.69 The committee therefore notes and agrees with the Department:

> Hardship variations cannot be listed as part of an individual's credit reporting information. The Government is concerned that permitting the listing of hardship variations may act as a deterrent to individuals seeking hardship variations in appropriate circumstances (including following a natural disaster) and this would be contrary to the intention of providing the right to request a hardship variation.[55]

Regulation of credit reporting

6.70 In relation to proposed new Part IIIA of the Privacy Act (item 72 of Schedule 2 of the Bill), the committee comments on various provisions as follows.

Permitted disclosures by credit reporting bodies and repayment history information

6.71 In her second reading speech, the Attorney-General noted that direct provision of 'repayment history information' will be restricted to 'credit providers' who are subject to responsible lending obligations under the National Consumer Credit Protection Act.[56] Proposed new section 20E of the Privacy Act (Use or disclosure of credit reporting information) gives effect to this policy proposal in relation to the disclosure of 'credit reporting information' by 'credit reporting bodies'.

6.72 The committee acknowledges the concerns of industry stakeholders which are not 'licensees' under the National Consumer Credit Protection Act. However, the committee notes:

> The purpose of the credit reporting system is to balance an individual's interests in protecting their personal information with the need to ensure sufficient personal information is available to assist a credit provider to

53 *Submission 29*, p. 6.

54 *Committee Hansard*, 10 August 2012, p. 31.

55 Answer to question on notice, received 3 September 2012, p. 15 (emphasis in the original).

56 *House of Representatives Hansard*, 23 May 2012, p. 5212.

> determine an individual's eligibility for credit following an application for credit by an individual, and for related matters.[57]

6.73 The committee also notes the proposed Objects of the Privacy Act (item 1 of Schedule 4 of the Bill) clause and, in particular, the first objective of promoting the privacy of individuals. In view of these objectives, the committee considers that it is appropriate to curtail the dissemination of individuals' 'repayment history information' even though its availability might be considered beneficial to, or more desirable for, certain sectors of the finance and credit industries.

6.74 On a separate matter, the committee acknowledges evidence provided by the Consumer Credit Legal Centre (NSW) indicating that the inclusion of 'repayment history information' in the credit reporting provisions of the Bill could be used to increase interest rates charged under a consumer credit contract. According to Ms Katherine Lane, this outcome would be detrimental to the most vulnerable of consumers in circumstances where they may have incurred only minor credit defaults.[58]

Use or disclosure of de-identified credit reporting information

6.75 Proposed new section 20M of the Privacy Act, preventing the use and disclosure of de-identified 'credit reporting information', also concerned several industry stakeholders. The committee heard arguments concerning the appropriateness of this provision and the value of de-identified data in the information economy.

6.76 A representative from the Department highlighted that the Bill has been drafted to prohibit all uses, disclosures and collections of personal information with permitted exceptions, including in relation to the secondary use of 'credit reporting information'. Further, the committee notes the Australian Government's express recognition of, and allowance for, 'research purposes that are deemed to be in the public interest and have a sufficient connection to the credit reporting system', subject to existing rules developed by the Office of the Australian Information Commissioner.[59]

6.77 The committee considers that it is appropriate for secondary uses of 'credit reporting information' to be regulated, particularly when it might be possible to re-identify the information.[60] The committee is not persuaded that proposed new section 20M will prevent industry from conducting relevant research activities and is of the view that there might also be merit in prohibiting the re-identification of

---

57 Explanatory Memorandum, p. 2.

58 *Submission 51*, p. 5.

59 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Draft of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 8.

60 EM, p. 144.

de-identified 'credit reporting information'[61] as an additional precautionary measure for the protection of individuals' personal information.

Recommendation 15

6.78 The committee recommends that the Australian Government consider prohibiting the re-identification of 'credit reporting information' which has been de-identified for research purposes in accordance with proposed new subsection 20M(2) in item 72 of Schedule 2 of the Bill, and whether a proportionate civil penalty should apply to any breach of that prohibition.

Correction of personal information and third party application

6.79 Proposed new subsections 20T(1) and 21V(1) (item 72 of Schedule 2) of the Privacy Act enable an individual to request the correction of certain personal information held by 'credit reporting bodies' and 'credit providers'. The committee notes that the entity concerned need not hold the disputed information, but will be required to deal with the correction request and assist the individual to have their personal information corrected.[62]

6.80 As noted by the Australasian Retail Credit Association, this requirement might be complex because of its focus on an operational process rather than an outcome.[63] The committee agrees that it might be more expedient for the recipient of a complaint to be able to refer a complainant to a more appropriate respondent; however, the committee is not persuaded that the Bill's proposed corrections process is unworkable. As suggested by the Office of the Australian Information Commissioner,[64] the process should be improved to strengthen its consumer protections.

Recommendation 16

6.81 The committee recommends that proposed new sections 20T and 21V in item 72 of Schedule 2 of the Bill be amended to:

- **create an obligation for the recipient of a request to take reasonable steps to have the information corrected by the entity which holds the disputed information;**
- **create an obligation for the entity which holds the disputed information to correct the information within 30 days, if satisfied that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; and**
- **create an obligation for the recipient of a request to notify the individual about the outcome of their request if that request has been determined by another entity which holds the disputed information.**

---

61 For example, see Australasian Retail Credit Association, *Submission 27*, p. 7.

62 EM, pp 148-149 and 180.

63 *Submission 27*, p. 11.

64 *Submission 47*, pp 23-24.

Correction of personal information and time to correct

6.82 The committee acknowledges the views of the Energy & Water Ombudsman NSW and the Telecommunications Industry Ombudsman, which argued that corrections to personal information should be made expeditiously.[65] The committee also notes the evidence of: the Australian Privacy Commissioner, Mr Timothy Pilgrim, who argued that where information is in dispute, the investigation leading to correction could well require more than the 30 days stipulated in proposed new subsections 20T(2) and 21V(2) (item 72 of Schedule 2) of the Privacy Act;[66] and consumer advocates, such as the Consumer Credit Legal Centre (NSW), which argued that, consistent with ALRC Recommendation 59-8, 'credit reporting bodies' and 'credit providers', should substantiate disputed listings within 30 days.[67]

6.83 In the circumstances, the committee considers that the 30-day timeframe is appropriate but an additional consumer protection would serve to prevent any possible prejudice to an individual while a corrections request is being investigated.[68]

Recommendation 17

6.84 The committee recommends that the regulations made pursuant to section 100 of the *Privacy Act 1988* provide a mechanism for 'credit reporting bodies' and 'credit providers' who have received a request for the correction of an individual's personal information to note on the individual's credit file that a correction is under investigation, with the notation to be removed upon completion of that investigation.

Correction of personal information and the concept of fairness

6.85 The Consumer Credit Legal Centre (NSW) highlighted that proposed new section 21V, and presumably also proposed new section 20T (both in item 72 of Schedule 2), does not allow for listings to be corrected in circumstances where a reasonable person would consider the listing to be unfair.[69] The committee believes that exceptional circumstances – such as natural disasters, bank error, fraud, medical incapacity, and mail theft – warrant such an allowance.

Recommendation 18

6.86 The committee recommends that the Bill be amended to enable a 'credit reporting body' or 'credit provider' to correct an individual's personal information in exceptional circumstances, such as in the case of natural disasters, bank error, fraud, medical incapacity, and mail theft.

---

65 *Submission 38,* p. 5 and *Submission 45,* p. 7, respectively.

66 *Committee Hansard*, 21 August 2012, p. 9.

67 *Submission 51*, p. 18.

68 Energy & Water Ombudsman NSW, *Submission 38,* p. 5.

69 *Submission 51*, p. 18.

Complaints procedures and third party issues

6.87 The committee notes the various concerns in relation to the complaints procedures in proposed new Division 5 of the credit reporting provisions. For example, the argument that the regime will prove impractical given the possibility of one entity needing to consult another entity about the complaint (proposed new subsection 23B(2); item 72 of Schedule 2).[70] Several stakeholders suggested that, to be effective, the Bill should allow the recipient of a complaint to refer a consumer to the entity which is the subject of the complaint.

6.88 The committee accepts the Department's evidence that the recipient of a complaint can refuse a complaint if it does not involve them,[71] and observes that the legislative provisions do not preclude the recipient of the complaint from referring a consumer to the appropriate entity.

Commencement

6.89 The committee received evidence from the finance and credit industries regarding the adequacy of lead time should the credit reporting reforms commence nine months after receiving Royal Assent. Submitters and witnesses expressed a range of views on alternative commencement dates, with suggestions ranging from 12-18 months calculated from specific points in the reform process to a date to be determined by the Attorney-General.

6.90 The committee notes that the Australian Government has engaged, and continues to engage, in extensive consultations with industry stakeholders regarding the reforms to Australia's privacy legislation. In the current inquiry, it was apparent that the number of contentious issues has been significantly reduced and the outstanding issues now under examination are quite specific.

6.91 In relation to the commencement date, the committee accepts the need for certainty in what has been a very lengthy and complex reform process. Noting the 2010-11 inquiries into the Exposure Drafts of the Bill by the Senate Finance and Public Administration Legislation Committee (F&PA committee), and the current public consultation in relation to the draft regulations, the committee considers that the proposed reforms are sufficiently advanced for industry to be well aware of the extent and nature of implementation measures required by the Bill.

6.92 The committee therefore accepts the Department's view that a commencement date of nine months is certain and appropriate.[72] The committee commends the Department for its acknowledgement of stakeholders' ongoing concerns;[73] however, the committee is of the view that, in the interests of certainty for all stakeholders, the commencement date should remain at nine months after Royal Assent.

---

70 Financial Ombudsman Service, *Submission 12*, p. 7.

71 Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 15.

72 Additional information, received 29 August 2012, p. 10.

73 Additional information, received 29 August 2012, pp 10-11.

Recommendation 19

6.93 The committee recommends that the commencement date for the Bill remain at nine months after the Bill receives Royal Assent in order to provide certainty for all relevant stakeholders.

6.94 As a final note, the committee observes that the Australian Government previously accepted the F&PA committee's recommendation to consult industry and consumers during the transitional phase of implementation.[74] The government's response also stated:

> The development of effective education and information resources by stakeholders and for stakeholders will be undertaken during the transition to the new regime. The Government anticipates that both industry and the Office of the Australian Information Commissioner…will play a significant role in providing education and assistance.[75]

6.95 The committee endorses this approach to raising public awareness and educating consumers about the impending privacy reforms.

Recommendation 20

6.96 The committee recommends that, before the Bill's commencement date, the Office of the Australian Information Commissioner – in consultation with the Attorney-General's Department, as appropriate – develop and publish material informing consumers of the key changes to privacy legislation as proposed by the Bill, and providing guidance to Commonwealth agencies and private sector organisations to ensure compliance with the new legislative requirements.

6.97 In conclusion, the committee commends the reform of Australia's privacy protection framework. The Bill represents one component of this reform and, while some specific amendments have been proposed by the committee, overall the committee supports the Bill and recommends its passage.

Recommendation 21

6.98 Subject to the preceding recommendations, the committee recommends that the Senate pass the Bill.

Senator Trish Crossin

Chair

---

74 Senate Finance and Public Administration Legislation Committee, *Exposure Draft of Australian Privacy Amendment Legislation, Part 2 – Credit Reporting*, October 2011, p. 49 (Recommendation 5).

75 Australian Government, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Draft of Australian Privacy Amendment Legislation: Part 2 – Credit Reporting*, May 2012, p. 4.

ADDITIONAL COMMENTS BY COALITION SENATORS

1.1 Coalition Senators are supportive of the need to reform Australia's privacy laws, to provide clarity and certainty and to enhance the privacy of citizens in many forms and media. But they are dismayed by the inept, ham-fisted way in which these reforms have been attempted in this bill.

1.2 Many of the submissions to this inquiry, and much of the evidence before the committee, were critical of the approach the government has taken to produce this legislation. Witnesses reported that the legislation had taken an inordinately long time to bring forward, that they and other stakeholders were substantially in the dark on the consultation process, that the provisions of the Bill were difficult to understand and that many provisions were so broadly or vaguely couched that much behaviour, which is currently considered acceptable in the marketplace, would be made unlawful in future. Some witnesses suggested the Bill was so bad it should be rejected outright by the Senate.[1]

1.3 The depth of the dismay obviously felt by many stakeholders stood in sharp contrast to the effusive, self-congratulatory language used by the Attorney-General in introducing the Bill.

1.4 Dr Anthony Bendall, the Acting Victorian Privacy Commissioner, said:

> Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life.[2]

1.5 Ms Katherine Lane, Principal Solicitor with the Consumer Credit Legal Centre (NSW) Inc, said of the Bill's readability and how well people were being prepared for their new rights and obligations:

> No, there has not been anything. Nothing at all. It is alarming...[E]very time I mention it to a client, they go white. They have no idea that any of this is coming. It will have a profound impact on the way they manage their household budget and their lives and their loans. Australia spends a huge amount of money on financial literacy, but we have not got anything happening on this.[3]

---

1 For example, Mr Nigel Waters, Australian Privacy Foundation, *Committee Hansard*, 21 August 2012, p. 48.

2 Joint Parliamentary Committee on Intelligence and Security, *Inquiry into potential reforms of the National Security Legislation*, Office of the Victorian Privacy Commissioner, *Submission 109*, p. 9.

3 *Committee Hansard*, 10 August 2012, p. 29.

1.6 The Law Council of Australia noted:

> [A] number of large penalties contained in the legislation are out of proportion to the gravity of the contraventions involved...[We regret] the availability of such significant penalties for events that may be trivial and may happen very quickly if an error arises.[4]

1.7 Mr Simon Remington, Managing Director of Remington Direct, said:

> [T]he inclusion of a 'prohibition on direct marketing' will cause considerable confusion with our clients as to whether direct marketing is permitted or not. This will have a direct, financial and reputation effect on our business…This decision would unquestionably cost many jobs within our industry plus within companies who use direct marketing to grow their business.[5]

1.8 The Australian Bankers' Association noted:

> [A]s far as the general privacy provisions are concerned, the proposed implementation timeframe in the Bill will be insufficient for our members to implement those reforms effectively.[6]

1.9 Faced with this avalanche of criticism, Coalition senators considered recommending that the Senate reject this legislation; however, we also note the predominant tone of stakeholder criticism, which is to the effect that: the Bill is deeply flawed, but privacy reform is urgent, so passing this package and fixing the problems later is the lesser of two evils.

1.10 Coalition Senators are broadly supportive of the committee majority's recommendations attempting to fix some of these problems. In other respects, we feel the report could go further at this time.

Direct marketing principle (APP 7)

1.11 APP 7.1 prohibits a private sector organisation which holds personal information about an individual from using or disclosing the information for the purpose of direct marketing. APP 7.2 and APP 7.3 provide exceptions to the general prohibition and are contingent upon an organisation providing a simple means by which an individual may easily request not to receive direct marketing communications from the organisation (APP 7.2(c) and APP 7.3(c)).

Breadth of the principle

1.12 Facebook, Google, IAB Australia and Yahoo!7 submitted that the proposed definition and application of 'direct marketing' would allow for an extremely broad application of the prohibition in APP 7.1. The joint submission stated that, in practice,

---

4 *Submission 14*, p. 12. Comment made in relation to penalties for contravention of credit reporting provisions.

5 *Submission 10*, p. 1.

6 *Submission 24*, p. 3.

this would prevent businesses providing any promotional communications to consumers and would potentially undermine ad-supported business models:

> This is so broad as to potentially cover all forms of communications between businesses and consumers that include any promotional material, including, for example, free-to-air television advertisements and free online, ad-supported services such as those offered by [us].[7]

1.13 Instead, Facebook, Google, IAB Australia and Yahoo!7 suggested an alternative definition of 'direct marketing' and 'direct marketing communication', which would allow consumers to continue to receive direct marketing in certain circumstances:[8]

> [T]he Proposed Law should not be read to (and we believe it is not intended to) permit a consumer to opt out of all direct marketing, if receiving direct marketing is part of the value exchange of the service that the consumer is choosing to receive. To avoid this ambiguity, APP 7.2 and APP 7.3 should be rephrased. APP7.2 and APP7.3 each require that an opt-out of direct marketing be provided. However it is not clear that the opt-out be from receipt of direct marketing *that relies on personal information.* Rather it is written as an opt-out of direct marketing altogether. In the event that 'direct marketing' were interpreted to include advertisements, this would undermine advertising based business models, which is surely not the intention of the [Bill].[9]

1.14 Coalition Senators note the Attorney-General's Department's (Department) response to this concern:

> APP 7 will not cover forms of direct marketing that are received by individuals that do not involve the use or disclosure of their personal information, such as where they are randomly targeted for generic advertising through a banner advertisement. Nor will APP 7 apply if it merely targets a particular internet address on an anonymous basis for direct marketing because of its web browsing history. These are current online direct marketing activities that will not be affected by the amendments.[10]

1.15 Coalition senators are not convinced, however, that the operational scope of APP 7, as drafted and explained in the Explanatory Memorandum, would be limited in this way. They note that the current business practice of these organisations, and presumably thousands like them, does entail harvesting personal information about,

---

7 *Submission 39*, p. 4. For a general discussion of how Facebook might approach operational inconsistencies with the Bill, see: Ms Samantha Yorke, IAB Australia, *Committee Hansard*, 10 August 2012, pp 37-38.

8 For example, a consumer could continue to receive a communication reasonably related to an ongoing service or customer relationship between the organisation and the individual, or a communication that a consumer has consented to receive.

9 *Submission 39*, pp 4-5 (emphasis in the original).

10 Additional information, received 29 August 2012, p. 2.

say, a subscriber's internet usage to direct incidental advertising to that subscriber's web account. Making such practices unlawful seems to repudiate widely used and well accepted marketing techniques, but the extent to which the Bill does so is far from clear.

1.16 Accordingly, Coalition Senators consider that either APP 7 or the Explanatory Memorandum should provide further clarification on this point to provide greater certainty for relevant private sector organisations.

Opt-out requirement

1.17 In evidence at the second public hearing, an officer of the Department elaborated on the application of APP 7, including the circumstances in which direct marketing using personal information is permitted:

> APP 7…sets up two situations for when people can use personal information for direct marketing. The first is essentially where there is an existing relationship with the customer, so the information has been collected from the customer and that customer has been provided with an opportunity to opt out of receiving direct marketing—essentially the point of collection. That is APP 7.2.
>
> The second situation is where information is being collected from somewhere other the person—from other information or from whatever source—and in that situation direct marketing can occur if, in relation to each instance of marketing, the individual is provided with the facility to opt out of receiving further direct marketing material. [That is APP 7.3].[11]

1.18 The departmental officer advised that the 'real intention' of APP 7.2 and APP 7.3 is to give consumers control over the use of their personal information in direct marketing.[12] However, Coalition Senators observe that there may be implementation difficulties, not just with the provision of a simple opt-out mechanism but also the requirement in APP 7.3(d), allowing for direct marketing if:

> (d) in each direct marketing communication with the individual:
>
> > (i) the organisation includes a prominent statement that the individual may make such a request; or
> >
> > (ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request[.][13]

1.19 Coalition Senators are of the view that, in a Bill intended to modernise a legislative framework, the proposed provisions should be not only practicable but should also, as far as possible, be 'future proofed' so that they can apply to current and future technologies in an international operating environment. The present provisions do appear to suffer from a lack of relevance to contemporary online practice.

---

11 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 7.

12 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 7.

13 For example, see: Fundraising Institute of Australia, *Submission 4*, p. 2; Australian Direct Marketing Association, *Submission 7*, p. 7.

1.20 Coalition Senators are concerned that APP 7.2 and APP 7.3 will be rendered meaningless if those provisions impose conditions which cannot be met for technical or logistical reasons. It is no answer to simply assert that private sector organisations must comply with what may be a practically impossible requirement.[14]

'Repayment history information' and lenders mortgage insurers

1.21 Proposed new subsection 20E(1) (item 72 of Schedule 2) of the Privacy Act prohibits a 'credit reporting body' which holds 'credit reporting information' about an individual from using or disclosing that information. There are a number of exceptions to this general prohibition (proposed new subsections 20E(2)-(3)); however, under proposed new subsection 20E(4) a 'credit reporting body' cannot disclose 'credit reporting information' derived from 'repayment history information' to recipients who are not 'licensees' under the *National Consumer Credit Protection Act 2009*, including, for example, lenders mortgage insurers (LMIs),[15] which are regulated by the Australian Prudential Regulation Authority.

1.22 The Insurance Council of Australia highlighted that LMIs assume the same risk as lenders:

> [I]mpeding their ability to assess this risk by denying direct access to the full range of credit information is likely to significantly affect the LMI providers' ability to actually provide LMI. This will impact on the availability and accessibility of borrowers (particularly first home buyers).[16]

1.23 Coalition Senators note that such an outcome would be contrary to some of the benefits of privacy reform identified by the Attorney-General in her second reading speech and, in particular, the enhanced ability of the finance and credit industry to make more accurate risk assessments.[17] Consistent with the introduction of more comprehensive credit reporting, Coalition Senators consider that, with the appropriate safeguards, there is no sound justification for disallowing LMIs from receiving 'credit reporting information' from a 'credit reporting body'.

Cross-border disclosures of personal information – 'Australian link'

1.24 Items 4 to 7 of Schedule 4 of the Bill amend the definition of 'Australian link' in subsections 5B(2) and 5B(3) of the Privacy Act. Coalition Senators note the intention of this amendment, as stated in the Explanatory Memorandum:

> The credit reporting system will not contain foreign credit information or information from foreign credit providers (even if they have provided credit to an individual who is in Australia), nor will information from the credit

14 Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 7.

15 Proposed new subsection 20E(4) of the Privacy Act (2,000 penalty units).

16 *Submission 23*, p. 2.

17 The Hon. Nicola Roxon MP, Attorney General, *House of Representatives Hansard*, 23 May 2012, pp 5211-5212.

> reporting system be available to foreign credit reporting bodies or foreign credit providers.[18]

1.25 The Explanatory Memorandum further indicates that the use of the term 'Australian link' throughout the credit reporting provisions in proposed new Part IIIA (item 72 of Schedule 2) of the Privacy Act was considered to be a simple, clear and effective approach to implementing the government's policy proposal.[19]

1.26 However, industry stakeholders gave evidence to the committee indicating that the use of the term 'Australian link' in proposed new section 21G (item 72 of Schedule 2)[20] of the Privacy Act will have an inadvertent and significant adverse effect on business operations. For example, Mrs Sue Jeffrey from the ANZ Banking Group Limited (ANZ) stated her company's position as follows:

> [T]he Australian link requirement will have a major effect on the way ANZ structures its businesses. For example, ANZ from time to time use credit assessment teams in New Zealand to assist with processing home loan applications during periods of high volume. We would like to retain this ability to move work across our geographies in order to best meet the needs of our customers. [The Bill] would represent a much more significant impact than we expect was intended. It would be a backward step in ANZ's ability to structure its operations in a way that supports our regional footprint and delivers our customers efficient, high quality service. At the same time it would offer no additional privacy protection to our customers.[21]

1.27 Mr Steven Münchenberg, representing the Australian Bankers' Association, told the committee that there was no reason why the 'Australian link' requirement should be so restrictive:

> ANZ have modelled their business in a particular way and other banks would have modelled theirs in different ways. Certainly [the Australian Bankers' Association] cannot see any reason why a wholly owned subsidiary in New Zealand should be banned from processing Australian data, nor can we see a reason why a company that has been set up in New Zealand to service New Zealand banks should not also be able to provide that service to Australian-based banks – as an example – provided, of course, they comply with either Australian standards or comparable standards in New Zealand...[W]e would certainly want to see this extended to agents.[22]

---

18 EM, p. 91.

19 EM, p. 91.

20 Proposed new section 21G prohibits the cross-border disclosure of 'credit eligibility information' by a 'credit reporting body', except in certain circumstances.

21 *Committee Hansard*, 10 August 2012, p. 15.

22 *Committee Hansard*, 10 August 2012, p. 19.

1.28 The Communications Alliance representative, Mr John Stanton, similarly referred to the application of the 'Australian link' requirement to service providers contracted by telecommunications providers:

> The implication for telecommunications companies that use contractors offshore for service activation and sales activities, activities which do require access to credit eligibility information, is that the Australian link requirement would make it very difficult for them to continue their work.[23]

1.29 The Department acknowledged that implementation of proposed new section 21G has caused unforeseen difficulties, which the Department is endeavouring to address.[24] In other words, this provision is anything but simple, clear and effective, and the Australian Government is asking the Senate to debate and pass the Bill without a solution in sight.

1.30 Coalition Senators can scarcely credit that an issue as serious as this was not identified and addressed much earlier than in the current inquiry. It also raises the question of what other oversights the Senate might be asked to scrutinise in the future, for example, conflict of laws arrangements necessitated by the Bill.

1.31 In the circumstances, therefore, Coalition Senators reserve the right to revisit their comments on the appropriateness and efficacy of the term 'Australian link' in the credit reporting provisions of Part IIIA of the Bill.

Use of de-identified credit reporting information

1.32 Witnesses argued that proposed section 20M was unnecessary, in that de-identified information cannot, by definition, be a breach of privacy. Coalition Senators agree. The regulation in the Bill of this kind of data seems a particularly pointless exercise in creating red tape. Coalition Senators note that the committee majority considers that 'it is appropriate for secondary uses of 'credit reporting information' to be regulated, particularly when it might be possible to re-identify the information', but no circumstances were brought to the committee's attention where such a situation could arise.

1.33 Coalition Senators believe this provision should be reconsidered.

Senator Gary Humphries **Senator Sue Boyce**

Deputy Chair

---

23 *Committee Hansard*, 10 August 2012, p. 16.

24 Additional information, received 29 August 2012, p. 6. Also see Mr Colin Minihan, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 2; Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 21 August 2012, p. 3.

ADDITIONAL COMMENTS BY THE AUSTRALIAN GREENS

1.1 The Australian Greens support the aims and objectives of the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (the Bill), in particular the unification of the National Privacy Principles and the Information Privacy Principles into the new Australian Privacy Principles that apply to both Commonwealth agencies and private sector organisations.

1.2 This Bill amends the *Privacy Act 1988* (Cth) (the Act) and has been developed following numerous reviews and inquiries, which have included significant consultations with stakeholders. However, as was pointed out during this inquiry process, the reforms have been a long-time coming; for example, this is the first major reform to credit reporting since its introduction in the 1990s.

1.3 While there was majority support for the contents of this Bill amongst stakeholders, some concerns were expressed that although this Bill did improve 'on the current position, and that is because it is an important step towards that goal of harmonisation and simplification' it could not necessarily be said 'that it was an enhancement'.[1] Indeed, three different stakeholders expressed some concerns that this Bill was a 'missed opportunity' as it did not go far enough in either streamlining provisions or providing consumers and citizens with better protections.[2]

1.4 Changes to Australian law to modernise, strengthen and streamline privacy and credit reporting provisions are important. In doing this, we need to be careful that we strike the right balance between privacy rights and the free flow of information.

1.5 The Australian Greens strongly support the strengthening of Australian law to ensure enhanced compatibility with our obligations under international human rights law. As a signatory to the International Covenant on Civil and Political Rights (ICCPR), Australia has an obligation to promote and protect the right to privacy. Article 17 of the ICCPR provides that:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

1.6 In signing up to the ICCPR, Australia has agreed to take all necessary steps to respect, protect and fulfil human rights.

---

1 Ms Miller, *Committee Hansard*, 21 August 2012, p. 45.

2 Ms Ganopolsky, Ms Miller and Professor Greenleaf, *Committee Hansard*, 21 August 2012, pp 46 and 51.

1.7 We agree with the findings and recommendations made by the Committee's Report and make the following additional comments, which are directed at improving consumer protection and privacy rights.

Repayment history provisions

1.8 Firstly, we agree with the objection to the repayment history provisions raised by the Consumer Credit Legal Centre (NSW) Inc (CCLC NSW). As CCLC NSW highlighted, the main reason for the repayment history provisions is that credit providers require this information so that they can deal with managing risk, including risk-based pricing. This will not result in positive outcomes for consumers as it may cause some consumers, particularly low income and disadvantaged consumers, to be faced with higher costs of credit.

1.9 The CCLC NSW highlighted that there is insufficient evidence to show that more comprehensive reporting will 'lead to decreased levels of over-indebtedness and lower credit default rates'.[3] Indeed, CCLC NSW contends that there is evidence that 'indebtedness increases with the introduction of more comprehensive credit reporting'.[4] Furthermore, CCLC NSW was very strongly opposed to the repayment history provisions for a number of additional reasons, including: their potential to entrench hardship; the lack of evidence to suggest that the current situation, which does not provide for repayment history to be made available, is causing any problems in the market; and, the likelihood they would lead to risk-based pricing, which will entrench disadvantage by leading to a higher cost of credit for those least able to afford it.[5]

1.10 The Australian Greens are concerned that while the repayment history provisions may benefit credit providers, they will not benefit vulnerable consumers and as a result we query the necessity of inclusion of these provisions in the Bill. We recommend that, in light of the evidence provided by consumer advocates, the Government reconsider inclusion of the fifth dataset relating to repayment history. If the Government decides to include more comprehensive credit reporting we are of the view that the Government should consider introducing better consumer protections to monitor and minimise the impact of this dataset, particularly so that consumers experiencing socio-economic disadvantage and poverty are not worse off. Various consumer advocates provided suggestions during the inquiry about how to do this, and in addition to those submissions we say that further thought should be given to better regulation and/or monitoring of credit providers and how they deal with risk-based pricing and its impact on vulnerable consumers.

---

3 Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, p. 3.

4 CCLC NSW, *Submission 51*, p. 5.

5 CCLC NSW, *Submission 51*, p. 5.

Definition of 'serious credit infringement'

1.11 The Australian Greens also agree with comments made by the Consumer Action Law Centre (CALC), and supported by CCLC NSW, that the 'amendment to the definition of 'serious credit infringement' at proposed section 6(1) will not address the serious problems that this definition creates'.[6] A serious credit infringement is, apart from bankruptcy, the most serious type of listing that can be made and it will ordinarily remain on a credit report for seven years. It is very significant and has substantial ramifications for individuals. It is therefore essential that such listings are proportionate to the type of credit infringement, and are accurate and based on clear evidence.

1.12 CALC expressed concerns with the amendment to the Bill that requires that a serious credit infringement cannot be listed unless six months has elapsed since the credit provider last had contact with the debtor. It appears that the intent of this change is to ensure that credit providers attempt to make contact with the debtor so as to avoid an incorrect listing. By its intent, the amendment seeks to enhance consumer protections. However, as CALC points out, there is no guarantee that this amendment will achieve its purported aim as the credit provider is not required to be proactive and attempt to make contact; the only requirement is that the credit provider waits six months before listing a serious credit infringement.

1.13 CALC referred to a previous submission by consumer advocates that the definition of 'serious credit infringement' should be replaced with two new definitions: 'un-contactable default' and a 'never paid' flag. CALC indicated that this would be 'a more effective and proportionate response'[7] and would involve the 'never paid' flag being removed after six months and converted to an 'un-contactable default'. Under an 'un-contactable default', if at any point the debtor contacts the creditor, this is re-categorised to a standard default. While we understand that a previous inquiry highlighted that this suggestion does not take into account the serious nature of intentional credit fraud, we say that further consideration should be given to improving this definition to encapsulate better consumer protections as suggested by CALC. If the Government feels that it is necessary to retain a listing that reflects the serious nature of intentional fraud, it could consider a system that allows for a 'fraudulent conduct' flag where there is clear and compelling documentary evidence, or conduct has been found to be fraudulent by a court of law.[8]

Timing of default listings

1.14 In relation to proposed paragraph 6Q(1), the Australian Greens are of the view that a default listing should not occur until at least 30 days after a default notice has been given. In practical terms, this gives a borrower sufficient time to receive the notice (which may be subject to the vagaries of the post), contact the credit provider and/or try to rectify a default before a listing can be made, and is consistent with other

6 CALC, *Submission 5*, p. 1.

7 CALC, *Submission 5*, p. 4.

8 CALC, *Submission 5*, p. 5.

credit laws. This recommendation was made by the CCLC NSW. The submission of the Australian Communications Consumer Action Network also suggested that a listing should not occur until the credit provider has made 'reasonable attempts' to contact the debtor and provided a 'specific warning' regarding the default listing.[9]

'Determinations' by the Australian Privacy Commissioner

1.15 Finally, we note significant concerns raised by the Australian Privacy Foundation (APF) and CCLC NSW regarding the lack of determinations that have been made under section 52 of the Act. As a result of this history, the APF is apprehensive about the effectiveness of new reform under section 96, which provides 'a right of appeal to the Administrative Appeals Tribunal against decisions by the Commissioner to make a 'determination' of a complaint under s 52(1) or (1A)'.[10] In its view, 'this new right of appeal is of little use unless complainants can require the Commissioner to make formal decisions under'[11] section 52 of the Act, and it recommends that:

> The Privacy Commissioner should be required to make a determination under s52 wherever a complainant so requests, and for complainants to be informed that they are entitled to such a formal resolution of their complaint.[12]

1.16 The Australian Law Reform Commission (ALRC) in its *Report 108: For your information – Australian privacy law and practice* made a similar recommendation in 2009.

1.17 The Office of the Australian Information Commissioner (OAIC) provided a supplementary submission to the inquiry and noted that the Government had specifically rejected the recommendation of the ALRC in 2009 on the ground that as an independent statutory officer the OAIC 'should be responsible for exercising the administrative decision making powers under the Privacy Act'.[13] While we understand the tension here, and the importance of promoting and respecting the independence of the OAIC, we believe it would be prudent for the Government to reconsider this matter and conduct a review of the functions and powers of the OAIC in relation to its system for managing complaints, conciliations and determinations.

---

9 Australian Communications Consumer Action Network, *Submission 50*, p. 7.

10 APF, *Submission 49*, p. 4.

11 APF, *Submission 49*, p. 5.

12 APF, *Submission 49*, p. 4.

13 OAIC, *Supplementary Submission 47*, pp 6-7.

Recommendation 1

1.18 The Government should reconsider inclusion of the fifth dataset relating to repayment history. If the Government decides to include more comprehensive credit reporting, it should also consider what additional consumer protections are necessary to monitor and minimise the impact of this dataset.

Recommendation 2

1.19 Further consideration should be given to improving the definition of 'serious credit infringement' with a view to enhancing consumer protections as suggested by CALC. If the Government is of the view that it is necessary to retain a listing that reflects the serious nature of intentional fraud, it should consider a system that allows for a 'fraudulent conduct' flag where there is clear and compelling documentary evidence, or conduct has been found to be fraudulent by a court of law.

Recommendation 3

1.20 Twelve months after the enactment of this Bill, the Government should conduct a review as to the effectiveness of the OAIC's system for managing complaints, conciliations and determinations.

Recommendation 4

1.21 Proposed new subsection 6Q(1) should be amended so as to require an appropriate amount of time, of at least 30 days, to have elapsed from the date that written notice is given before a default listing is made.

Senator Penny Wright
Australian Greens

APPENDIX 1
AUSTRALIAN PRIVACY PRINCIPLES

Schedule 1—Australian Privacy Principles

Overview of the Australian Privacy Principles

Overview

This Schedule sets out the Australian Privacy Principles.

Part 1 sets out principles that require APP entities to consider the privacy of personal information, including ensuring that APP entities manage personal information in an open and transparent way.

Part 2 sets out principles that deal with the collection of personal information including unsolicited personal information.

Part 3 sets out principles about how APP entities deal with personal information and government related identifiers. The Part includes principles about the use and disclosure of personal information and those identifiers.

Part 4 sets out principles about the integrity of personal information. The Part includes principles about the quality and security of personal information.

Part 5 sets out principles that deal with requests for access to, and the correction of, personal information.

Australian Privacy Principles

The Australian Privacy Principles are:

Australian Privacy Principle 1—open and transparent management of personal information

Australian Privacy Principle 2—anonymity and pseudonymity

Australian Privacy Principle 3—collection of solicited personal information

Australian Privacy Principle 4—dealing with unsolicited personal information

Australian Privacy Principle 5—notification of the collection of personal information

Australian Privacy Principle 6—use or disclosure of personal information

Australian Privacy Principle 7—direct marketing

Australian Privacy Principle 8—cross-border disclosure of personal information

Part 1—Consideration of personal information privacy

1 Australian Privacy Principle 1—open and transparent management of personal information

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and

(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(f) whether the entity is likely to disclose personal information to overseas recipients;

(g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

2 Australian Privacy Principle 2—anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or

(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves.

Part 2—Collection of personal information

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

4 Australian Privacy Principle 4—dealing with unsolicited personal information

4.1 If:

(a) an APP entity receives personal information; and

(b) the entity did not solicit the information;

the entity must, within a reasonable period after receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.

4.2 The APP entity may use or disclose the personal information for the purposes of making the determination under subclause 4.1.

4.3 If:

(a) the APP entity determines that the entity could not have collected the personal information; and

(b) the information is not contained in a Commonwealth record;

the entity must, as soon as practicable but only if it is lawful and reasonable to do so, destroy the information or ensure that the information is de-identified.

4.4 If subclause 4.3 does not apply in relation to the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had collected the information under Australian Privacy Principle 3.

5 Australian Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Part 3—Dealing with personal information

6 Australian Privacy Principle 6—use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the ***primary purpose***), the entity must not use or disclose the information for another purpose (the ***secondary purpose***) unless:

(a) the individual has consented to the use or disclosure of the information; or

(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.

Note: Australian Privacy Principle 8 sets out requirements for the disclosure of personal information to a person who is not in Australia or an external Territory.

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:

(i) if the information is sensitive information—directly related to the primary purpose; or

(ii) if the information is not sensitive information—related to the primary purpose; or

(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(c) a permitted general situation exists in relation to the use or disclosure of the information by the APP entity; or

(d) the APP entity is an organisation and a permitted health situation exists in relation to the use or disclosure of the information by the entity; or

(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.

6.3 This subclause applies in relation to the disclosure of personal information about an individual by an APP entity that is an agency if:

(a) the agency is not an enforcement body; and

(b) the information is biometric information or biometric templates; and

(c) the recipient of the information is an enforcement body; and

(d) the disclosure is conducted in accordance with the guidelines made by the Commissioner for the purposes of this paragraph.

6.4 If:

(a) the APP entity is an organisation; and

(b) subsection 16B(2) applied in relation to the collection of the personal information by the entity;

the entity must take such steps as are reasonable in the circumstances to ensure that the information is de-identified before the entity discloses it in accordance with subclause 6.1 or 6.2.

Written note of use or disclosure

6.5 If an APP entity uses or discloses personal information in accordance with paragraph 6.2(e), the entity must make a written note of the use or disclosure.

Related bodies corporate

6.6 If:

(a) an APP entity is a body corporate; and

(b) the entity collects personal information from a related body corporate;

this principle applies as if the entity's primary purpose for the collection of the information were the primary purpose for which the related body corporate collected the information.

Exceptions

6.7 This principle does not apply to the use or disclosure by an organisation of:
(a) personal information for the purpose of direct marketing; or
(b) government related identifiers.

7 Australian Privacy Principle 7—direct marketing

Prohibition on direct marketing

7.1 If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Exceptions—personal information other than sensitive information

7.2 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:
(a) the organisation collected the information from the individual; and
(b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and
(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
(d) the individual has not made such a request to the organisation.

7.3 Despite subclause 7.1, an organisation may use or disclose personal information (other than sensitive information) about an individual for the purpose of direct marketing if:
(a) the organisation collected the information from:
(i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or
(ii) someone other than the individual; and
(b) either:
(i) the individual has consented to the use or disclosure of the information for that purpose; or
(ii) it is impracticable to obtain that consent; and
(c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
(d) in each direct marketing communication with the individual:
(i) the organisation includes a prominent statement that the individual may make such a request; or
(ii) the organisation otherwise draws the individual's attention to the fact that the individual may make such a request; and
(e) the individual has not made such a request to the organisation.

Exception—sensitive information

7.4 Despite subclause 7.1, an organisation may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

Exception—contracted service providers

7.5 Despite subclause 7.1, an organisation may use or disclose personal information for the purpose of direct marketing if:

(a) the organisation is a contracted service provider for a Commonwealth contract; and

(b) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract; and

(c) the use or disclosure is necessary to meet (directly or indirectly) such an obligation.

Individual may request not to receive direct marketing communications etc.

7.6 If an organisation (the ***first organisation***) uses or discloses personal information about an individual:

(a) for the purpose of direct marketing by the first organisation; or

(b) for the purpose of facilitating direct marketing by other organisations;

the individual may:

(c) if paragraph (a) applies—request not to receive direct marketing communications from the first organisation; and

(d) if paragraph (b) applies—request the organisation not to use or disclose the information for the purpose referred to in that paragraph; and

(e) request the first organisation to provide its source of the information.

7.7 If an individual makes a request under subclause 7.6, the first organisation must not charge the individual for the making of, or to give effect to, the request and:

(a) if the request is of a kind referred to in paragraph 7.6(c) or (d)—the first organisation must give effect to the request within a reasonable period after the request is made; and

(b) if the request is of a kind referred to in paragraph 7.6(e)—the organisation must, within a reasonable period after the request is made, notify the individual of its source unless it is impracticable or unreasonable to do so.

Interaction with other legislation

7.8 This principle does not apply to the extent that any of the following apply:

(a) the *Do Not Call Register Act 2006*;

(b) the *Spam Act 2003*;

(c) any other Act of the Commonwealth, or a Norfolk Island enactment, prescribed by the regulations.

8 Australian Privacy Principle 8—cross-border disclosure of personal information

8.1 Before an APP entity discloses personal information about an individual to a person (the ***overseas recipient***):

(a) who is not in Australia or an external Territory; and

(b) who is not the entity or the individual;

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

(a) the entity reasonably believes that:

(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and

(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or

(b) both of the following apply:

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) the disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the disclosure of the information by the APP entity; or

(e) the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing to which Australia is a party; or

(f) the entity is an agency and both of the following apply:

(i) the entity reasonably believes that the disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body;

(ii) the recipient is a body that performs functions, or exercises powers, that are similar to those performed or exercised by an enforcement body.

9 Australian Privacy Principle 9—adoption, use or disclosure of government related identifiers

Adoption of government related identifiers

9.1 An organisation must not adopt a government related identifier of an individual as its own identifier of the individual unless:

(a) the adoption of the government related identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(b) subclause 9.3 applies in relation to the adoption.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Use or disclosure of government related identifiers

9.2 An organisation must not use or disclose a government related identifier of an individual unless:

(a) the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions; or

(b) the use or disclosure of the identifier is reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or

(c) the use or disclosure of the identifier is required or authorised by or under an Australian law or a court/tribunal order; or

(d) a permitted general situation (other than the situation referred to in item 4 or 5 of the table in subsection 16A(1)) exists in relation to the use or disclosure of the identifier; or

(e) the organisation reasonably believes that the use or disclosure of the identifier is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(f) subclause 9.3 applies in relation to the use or disclosure.

Note: An act or practice of an agency may be treated as an act or practice of an organisation, see section 7A.

Regulations about adoption, use or disclosure

9.3 This subclause applies in relation to the adoption, use or disclosure by an organisation of a government related identifier of an individual if:

(a) the identifier is prescribed by the regulations; and

(b) the organisation is prescribed by the regulations, or is included in a class of organisations prescribed by the regulations; and

(c) the adoption, use or disclosure occurs in the circumstances prescribed by the regulations.

Note: There are prerequisites that must be satisfied before the matters mentioned in this subclause are prescribed, see subsections 100(2) and (3).

Part 4—Integrity of personal information

10 Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

11 Australian Privacy Principle 11—security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

11.2 If:

(a) an APP entity holds personal information about an individual; and

(b) the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule; and

(c) the information is not contained in a Commonwealth record; and

(d) the entity is not required by or under an Australian law, or a court/tribunal order, to retain the information;

the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Part 5—Access to, and correction of, personal information

12 Australian Privacy Principle 12—access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exception to access—agency

12.2 If:

(a) the APP entity is an agency; and

(b) the entity is required or authorised to refuse to give the individual access to the personal information by or under:

(i) the Freedom of Information Act; or

(ii) any other Act of the Commonwealth, or a Norfolk Island enactment, that provides for access by persons to documents;

then, despite subclause 12.1, the entity is not required to give access to the extent that the entity is required or authorised to refuse to give access.

Exception to access—organisation

12.3 If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:

(a) the entity reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or

(b) giving access would have an unreasonable impact on the privacy of other individuals; or

(c) the request for access is frivolous or vexatious; or

(d) the information relates to existing or anticipated legal proceedings between the entity and the individual, and would not be accessible by the process of discovery in those proceedings; or

(e) giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(f) giving access would be unlawful; or

(g) denying access is required or authorised by or under an Australian law or a court/tribunal order; or

(h) both of the following apply:

(i) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in;

(ii) giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or

(i) giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or

(j) giving access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process.

Dealing with requests for access

12.4 The APP entity must:

(a) respond to the request for access to the personal information:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so.

Other means of access

12.5 If the APP entity refuses:

(a) to give access to the personal information because of subclause 12.2 or 12.3; or

(b) to give access in the manner requested by the individual;

the entity must take such steps (if any) as are reasonable in the circumstances to give access in a way that meets the needs of the entity and the individual.

12.6 Without limiting subclause 12.5, access may be given through the use of a mutually agreed intermediary.

Access charges

12.7 If the APP entity is an agency, the entity must not charge the individual for the making of the request or for giving access to the personal information.

12.8 If:

(a) the APP entity is an organisation; and

(b) the entity charges the individual for giving access to the personal information;

the charge must not be excessive and must not apply to the making of the request.

Refusal to give access

12.9 If the APP entity refuses to give access to the personal information because of subclause 12.2 or 12.3, or to give access in the manner requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

12.10 If the APP entity refuses to give access to the personal information because of paragraph 12.3(j), the reasons for the refusal may include an explanation for the commercially sensitive decision.

13 Australian Privacy Principle 13—correction of personal information

Correction

13.1 If:

(a) an APP entity holds personal information about an individual; and

(b) either:

(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading; or

(ii) the individual requests the entity to correct the information;

the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete, relevant and not misleading.

Notification of correction to third parties

13.2 If:

(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and

(b) the individual requests the entity to notify the other APP entity of the correction;

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

Refusal to correct information

13.3 If the APP entity refuses to correct the personal information as requested by the individual, the entity must give the individual a written notice that sets out:

(a) the reasons for the refusal except to the extent that it would be unreasonable to do so; and

(b) the mechanisms available to complain about the refusal; and

(c) any other matter prescribed by the regulations.

Request to associate a statement

13.4 If:

(a) the APP entity refuses to correct the personal information as requested by the individual; and

(b) the individual requests the entity to associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant or misleading;

the entity must take such steps as are reasonable in the circumstances to associate the statement in such a way that will make the statement apparent to users of the information.

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

(a) must respond to the request:

(i) if the entity is an agency—within 30 days after the request is made; or

(ii) if the entity is an organisation—within a reasonable period after the request is made; and

(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).

APPENDIX 2

SUBMISSIONS RECEIVED

Submission Number	Submitter
1	Epworth HealthCare
2	Australian Medical Association
3	Queensland Law Society
4	Fundraising Institute Australia
5	Consumer Action Law Centre (NSW)
6	Consumer Credit Legal Service Western Australia
7	Australian Direct Marketing Association
8	Law Institute of Victoria
9	Magnamail
10	Remington Direct
11	Pareto Phone and Pareto Fundraising
12	Financial Ombudsman Service
13	Liberty Victoria
14	Law Council of Australia
15	The Mailing House
16	Australian Industry Group
17	Office of the Victorian Privacy Commissioner

18	Confidential
19	Australian Broadcasting Corporation
20	Confidential
21	Foxtel
22	Centre for Internet Safety
23	Insurance Council of Australia
24	Australian Bankers' Association
25	Abacus-Australian Mutuals
26	Salmat Limited
27	Australasian Retail Credit Association
28	Diners Club International
29	ANZ Banking Group Limited
30	Communications Alliance
31	Optus
32	Acxiom Australia
33	Hunter Community Legal Centre
34	Commercial Asset Finance Brokers Association of Australia
35	Experian Australia Credit Services
36	Australian Finance Conference
37	GEON

38	Energy and Water Ombudsman NSW
39	Facebook, Google, IAB Australia and Yahoo!7
40	Yahoo!7
41	Veda
42	NSW Privacy Commissioner
43	GE Capital
44	Dun & Bradstreet, Experian and Veda
45	Telecommunications Industry Ombudsman
46	Kimberly-Clark Australia
47	Office of the Australian Information Commissioner
48	Min-it Software
49	Australian Privacy Foundation
50	Australian Communications Consumer Action Network
51	Consumer Credit Legal Centre (NSW)
52	Telstra
53	Australian Association of National Advertisers
54	Confidential
55	NSW Department of Attorney General and Justice
56	Finance Industry Delegation
57	Name Withheld

58 Greater Data

59 Vodafone

ADDITIONAL INFORMATION RECEIVED

1 Material tabled by Veda at public hearing on 10 August 2012

2 Document tabled by Veda at public hearing on 10 August 2012 – Quarterly Consumer Credit Demand Index, April-June 2012

3 Additional information provided by Australasian Retail Credit Association on 13 August 2012 – Policy and Economic Research Council, Credit Impact of More Comprehensive Credit Reporting in Australia and New Zealand

4 Response to questions on notice provided by Australian Direct Marketing Association on 23 August 2012

5 Response to questions on notice provided by Communications Alliance on 23 August 2012

6 Response to questions on notice provided by Facebook, Google, IAB Australia and Yahoo!7 on 23 August 2012

7 Response to questions on notice provided by Law Institute of Victoria on 23 August 2012

8 Response to questions on notice provided by Consumer Credit Legal Centre (NSW) on 23 August 2012

9 Response to questions on notice provided by Financial Ombudsman Service on 23 August 2012

10 Response to questions on notice provided by Australasian Retail Credit Association on 24 August 2012

11 Additional information provided by Attorney-General's Department on 29 August 2012

12 Response to questions on notice provided by ANZ Banking Group Limited on 29 August 2012

13 Response to questions on notice provided by Australian Bankers' Association on 29 August 2012

14 Additional information provided by Attorney-General's Department on 3 September 2012

15 Responses to questions on notice provided by Attorney-General's Department on 3 and 14 September 2012

APPENDIX 3

WITNESSES WHO APPEARED BEFORE THE COMMITTEE

Canberra, 10 August 2012

AHLIN, Mr Sam, Principal Legal Officer, Business and Information Law Branch, Attorney-General's Department

BOND, Ms Carolyn, Co-Chief Executive Officer, Consumer Action Law Centre

BOOTH, Ms Sharon, Head of Compliance, Australia and New Zealand, Experian Asia Pacific Pty Ltd

BROWN, Mr Steven, Director, Consumer Risk Solutions, Dun & Bradstreet

FALK, Ms Angelene, Director, Policy, Office of the Australian Information Commissioner

FIELD, Mr Philip, Ombudsman, Banking and Finance, Financial Ombudsman Service

GANOPOLSKY, Ms Olga, Chair, Business Law Section, Privacy Committee, Law Council of Australia

GIJSELMAN, Mr Matt, Chief Industry Advisor, Australasian Retail Credit Association

GLENN, Mr Richard, Assistant Secretary, Business and Information Law Branch, Attorney-General's Department

GRAFTON, Dr David, Executive General Manager, Credit and Marketing Solutions Group, Veda

GREENLEAF, Professor Graham, Board Member, Australian Privacy Foundation

JEFFREY, Mrs Sue, Acting General Manager, Australian Operations, ANZ Banking Group Limited

JENKINS, Ms Kim, Managing Director, Australia and New Zealand, Experian Asia Pacific Pty Ltd

LANE, Ms Katherine, Principal Solicitor, Consumer Credit Legal Centre (NSW)

McCRIMMON, Professor Les

MILLER, Ms Katie, Council Member, Law Institute of Victoria

MÜNCHENBERG, Mr Steven, Chief Executive Officer, Australian Bankers' Association

NASH, Ms Jane, Head of Financial Inclusion, ANZ Banking Group Limited

NIVEN, Mr David, Legal Counsel, Financial Ombudsman Service

PARMETER, Mr Nicholas, Manager, Civil Justice Division, Law Council of Australia

PAULL, Mr Damian, Chief Executive Officer, Australasian Retail Credit Association

PILGRIM, Mr Timothy, Australian Privacy Commissioner, Office of the Australian Information Commissioner

SANGSTER, Ms Jodie, Chief Executive Officer, Australian Direct Marketing Association

STANTON, Mr John, Chief Executive Officer, Communications Alliance

STRASSBERG, Mr Matthew, Senior Adviser, External Relations, Veda

WATERS, Mr Nigel, Public Officer and Policy Coordinator, Australian Privacy Foundation

YORKE, Ms Samantha, Director of Regulatory Affairs, IAB Australia

Canberra, 21 August 2012

AHLIN, Mr Sam, Principal Legal Officer, Business and Information Law Branch, Attorney-General's Department

FALK, Ms Angelene, Director, Policy, Office of the Australian Information Commissioner

GLENN, Mr Richard, Assistant Secretary, Business and Information Law Branch, Attorney-General's Department

MINIHAN, Mr Colin, Principal Legal Officer, Business and Information Law Branch, Attorney-General's Department

PILGRIM, Mr Timothy, Australian Privacy Commissioner, Office of the Australian Information Commissioner