
The Parliament of the Commonwealth of Australia

Advisory Report

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

House of Representatives
Standing Committee on Social Policy and Legal Affairs

September 2012
Canberra

© Commonwealth of Australia 2012

ISBN 978-0-642-79790-2 (Printed version)

ISBN 978-0-642-79791-9 (HTML version)

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Australia License.



The details of this licence are available on the Creative Commons website:

<http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.



Contents

Membership of the Committee	v
Terms of reference	vii
List of acronyms	ix
List of recommendations	xi

THE REPORT

1 Introduction	1
Scope of the Bill	1
Referral of the Bill	2
Previous inquiries and consultation	2
Concurrent Senate inquiry	3
Conduct and scope of this inquiry	3
Structure of the report	5
2 Australian Privacy Principles.....	7
Defences to contravention of APP 8	7
Compliance with overseas laws	11
Direct marketing.....	12
‘Opt out’ provisions for direct marketing.....	14
Committee comment.....	15
3 Credit Reporting Provisions	17
The Australian link requirement	17
Repayment history data provisions	21

Addresses stored on file 23

Committee Comment 24

4 Further issues.....27

 De-identified data 27

 Commencement period 29

 Complexity..... 31


 Committee comment..... 32

 Concluding remarks 33

APPENDICES

Appendix A – List of Submissions37

Appendix B – List of Witnesses Appearing at Public Hearing41



Membership of the Committee

Chair Mr Graham Perrett MP

Deputy Chair The Hon. Judi Moylan MP

Members Mr Shayne Neumann MP

The Hon. Dr Sharman Stone MP

Mr Ross Vasta MP

Ms Laura Smyth MP

Mr Mike Symon MP (to 14/08/12)

Ms Michelle Rowland MP (from 14/08/12)

Committee Secretariat

Secretary

Dr Anna Dacre

Research Officer

Ms Zoe Scanlon



Terms of reference

On 24 May 2012 the Selection Committee of the House of Representatives referred the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 for inquiry and report.



List of acronyms

ABA	Australian Bankers' Association
ADMA	Australian Direct Marketing Association
ALRC	Australian Law Reform Commission
ANZ	Australia and New Zealand Banking Group Limited
APF	Australian Privacy Foundation
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulation Authority
ARCA	Australasian Retail Credit Association
CCLC	Consumer Credit Legal Centre, New South Wales
CR Code	Credit Reporting Code
FACTA	US Foreign Accounts Tax Compliance Act 2010
GE	General Electric Capital
IPPs	Information Privacy Principles
LCA	Law Council of Australia
NPPs	National Privacy Principles
OAIC	Office of the Australian Information Commissioner
OPCNSW	Office of the Privacy Commissioner, New South Wales



List of recommendations

Recommendation 1

The Committee recommends that the House of Representatives pass the Privacy Amendment (Enhancing Privacy Protections) Bill 2012.

Recommendation 2

The Committee recommends that the Attorney-General agree to conduct a review of the Privacy Amendment (Enhancing Privacy Protections) Bill 2012 twelve months after the commencement of the Act, addressing the following issues:

- Defence to contravention of APP 8
- Conflicting overseas laws
- Direct marketing and opt out provisions for direct marketing
- De-identified data provisions
- The system regulating/preventing credit reporting information overseas (the Australian link requirement), and
- The effect of the repayment history provisions on addresses stored on file.

Recommendation 3

The Committee recommends that the Attorney-General ensure that comprehensive educational material on the new privacy protections and obligations is available prior to commencement of the Act.

Introduction

- 1.1 The Privacy Amendment (Enhanced Privacy Protection) Bill 2012 (hereafter referred to as the Privacy Amendment Bill) was introduced into the House of Representatives on 23 May 2012.

Scope of the Bill

- 1.2 The Privacy Amendment Bill will amend the *Privacy Act 1988* (Cth) and was developed in response to the Australian Law Reform Commission's (ALRC) 2008 report resulting from its inquiry into Australia's privacy laws.¹ The ALRC made 295 recommendations, which the Government has announced it intends to respond to in two stages.² This Bill is the first stage response and addresses 197 of the ALRC's recommendations.³
- 1.3 The Bill will create the Australian Privacy Principles (APPs) to replace the National Privacy Principles (NPPs) and the Information Privacy Principles (IPPs), which currently apply to the private and public sectors respectively. The APPs are a set of unified principles that will apply to both sectors. The changes are intended to bring greater clarity and consistency to Australia's privacy laws and more comprehensive privacy protection.
- 1.4 The Bill will also introduce a more comprehensive credit reporting system. The new measures will replace the current measures in their entirety and aim to introduce greater simplicity, clarity and consistency. They also aim

1 Privacy Amendment (Enhanced Privacy Protection) Bill 2012, Explanatory Memorandum.

2 Privacy Amendment (Enhanced Privacy Protection) Bill 2012, Explanatory Memorandum.

3 Privacy Amendment (Enhanced Privacy Protection) Bill 2012, Explanatory Memorandum.

to operate more effectively in light of developments in the way the system operates since its introduction.

- 1.5 The Bill includes provisions on a code system which allows customised privacy codes to be developed by organisations or industries. It also allows the Privacy Commissioner to develop and register binding codes in the public interest in some circumstances. The Bill also includes provisions governing the credit reporting code.
- 1.6 The Bill will clarify the powers of the Privacy Commissioner and is intended to improve the Commissioner's ability to deal with complaints, conduct investigations, make use of external dispute resolution services and promote compliance with the APPs.

Referral of the Bill

- 1.7 On 24 May 2012 the Selection Committee referred the Privacy Amendment Bill to the House of Representatives Standing Committee on Social Policy and Legal Affairs for inquiry and report.
- 1.8 The Selection Committee provided the following reasons for referral/principal issues for consideration:
- the adequacy of the proposed Australian Privacy Principles
 - the efficacy of the proposed measures relating to credit reporting
 - whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections, and
 - whether provisions relating to use of depersonalised data are appropriate.⁴

Previous inquiries and consultation

- 1.9 The ALRC undertook a 28 month inquiry in Australia's privacy laws and in 2008, produced a report of its findings (the ALRC report) including 295 recommendations for reform.⁵

4 House of Representatives Selection Committee, *Report 53*, 24 May 2012.

5 ALRC, *For your Information: Australian Privacy Law and Practice (ALRC Report 108)*, August 2008.

- 1.10 The Australian Government released its first stage response to the ALRC report in October 2009, including exposure drafts of the APPs and the credit reporting provisions. These exposure drafts were tabled in the Senate.
- 1.11 On 24 June 2010, the Senate referred the exposure drafts to the Senate Standing Committee on Finance and Public Administration for inquiry and report.
- 1.12 In June 2011, the Standing Committee on Finance and Public Administration tabled its report on the exposure draft of the APPs. In October 2011, it tabled its report on the exposure draft of the credit reporting provisions.⁶

Concurrent Senate inquiry

- 1.13 On 19 June 2012 the Senate referred the Privacy Amendment Bill to the Senate Standing Committee on Legal and Constitutional Affairs for inquiry and report.
- 1.14 The Senate Committee issued a call for submissions and received over 50 submissions from a range of individuals and organisations across Australia. Public hearings were conducted on 10 August and 21 August 2012. Submissions, transcripts and the Committee's report can be accessed on the Senate's website.⁷

Conduct and scope of this inquiry

- 1.15 The House Standing Committee on Social Policy and Legal Affairs advertised a public hearing and a call for submissions in *The Australian* newspaper on 11 July and 8 August 2012.
- 1.16 The Committee received 39 submissions and six supplementary submissions from a range of individuals and organisations across

6 Senate Standing Committee on Finance and Public Administration, *Exposure Drafts of Australian Privacy Amendment Legislation*, June 2011.

7 Senate Standing Committee on Legal and Constitutional Affairs, <http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Committees?url=legcon_ctte/index.htm>, accessed 5 September 2012.

Australia. These submissions are listed at Appendix A and can be accessed from the inquiry website.⁸

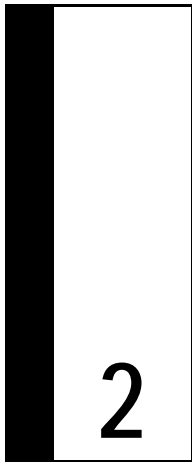
- 1.17 The Committee held a public hearing on 16 August 2012.⁹ A list of witnesses that appeared before the Committee is at Appendix B.
- 1.18 The Committee notes that this is an extremely complex inquiry. The Privacy Amendment Bill and its accompanying Explanatory Memorandum are both lengthy, complex documents and implement an intricate and comprehensive privacy regime. Privacy laws govern many facets of Australian life and the Committee appreciates that these changes will affect not only every Australian in their individual capacity but a wide variety of industries and organisations who hold personal information as part of their business activities.
- 1.19 The submissions the Committee received raised a multitude of issues. The Committee has not attempted to examine all these issues in detail, nor report on each comprehensively.
- 1.20 The Committee is aware that, while significant consultation was undertaken in the preparation of the Privacy Amendment Bill, there remain a number of outstanding concerns from industry and consumers. The Committee acknowledges the breadth of these concerns but has chosen to focus on those concerns it considers the most significant and those that have been raised repeatedly in submissions to this inquiry.
- 1.21 The Committee has endeavoured to acknowledge the majority of issues raised, however the implementation of a privacy regime will necessarily involve an assessment of balancing the protection of privacy rights while allowing for the convenient flow of data. The Committee's objective has been to evaluate the success of this Bill in achieving that balance.
- 1.22 This Bill has also been examined by the Senate Standing Committee on Legal and Constitutional Affairs. As far as possible, this Committee has endeavoured not to duplicate those areas it anticipates the Senate will consider in detail. Therefore, in some instances the Committee refers to the evidence and discussion in the Senate inquiry.

8 House of Representatives Standing Committee on Social Policy and Legal Affairs, <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=spla/bill%20privacy/index.htm>, accessed 5 September 2012

9 House of Representatives Standing Committee on Social Policy and Legal Affairs, <http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=spla/bill%20privacy/index.htm>, accessed 5 September 2012.

Structure of the report

- 1.23 Chapter Two considers APPs, notably defences to contravention of APP 8, compliance with overseas laws, direct marketing and the 'opt out' provisions for direct marketing.
- 1.24 Chapter Three considers credit reporting provisions, particularly the Australia link requirement, repayment history data provisions and the storage of addresses on file.
- 1.25 Chapter Four considers a number of additional issues, including de-identified data, the commencement period and the complexity of the regime.



Australian Privacy Principles

- 2.1 The Australian Privacy Principles (APPs) are contained in Schedule 1 of the Privacy Amendment Bill. The principles cover:
- transparent management of personal information
 - the collection, use and disclosure of personal information
 - identifiers, integrity, quality and security of personal information, and
 - access to and correction of personal information.

Defences to contravention of APP 8

- 2.2 Proposed APP 8.1 requires an entity disclosing personal information to an overseas recipient to take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to that information.
- 2.3 Proposed section 16C outlines certain circumstances in which an act done by the overseas recipient can be taken to be a breach of the APPs by the disclosing Australian entity.
- 2.4 A number of exceptions to APP 8.1 exist:
- where the entity has a reasonable belief that the overseas recipient is bound by legal or binding obligations to protect information in a similar way to the protection provided by the APPs¹

¹ Proposed APP 8.2(a).

- where an individual consents to the cross-border disclosure, after being informed that the consequence of giving their consent is that the requirement in APP 8.1 will not apply²
 - where the disclosure is required or authorised by law³
 - where limited 'permitted general situations' exist (in proposed section 16A(1))⁴
 - where the disclosure is required or authorised by or under an international agreement relating to information sharing, the entity is an agency and Australia is party to that agreement,⁵ and
 - where the entity is an agency, and the agency reasonably believes that the disclosure is reasonably necessary for enforcement related activities by an enforcement body and the overseas recipient's functions are similar to those of an enforcement body.⁶
- 2.5 The Australian Law Reform Commission (ALRC) inquired in some depth into ideal arrangements for the cross border disclosure of data flows⁷ but did not closely consider the question of defences or how any such defences should be framed. Consequently, the ALRC has not formed a view on this issue.⁸
- 2.6 Many submissions express concern that holding the disclosing Australian organisation responsible for a breach that occurs overseas places too great a burden on organisations that regularly transfer data overseas.⁹
- 2.7 Foxtel expressed concern that even where an organisation takes reasonable steps, such as reviewing its security controls, it may still be found liable for a data breach that occurred overseas, even where access to the information is unauthorised, such as a hacking situation.¹⁰

2 Proposed APP 8.2(b).

3 Proposed APP 8.2(c).

4 Proposed APP 8.2(d).

5 Proposed APP 8.2(e).

6 Proposed APP 8.2(f).

7 ALRC, *For Your Information: Australian Privacy Law and Practice (ALRC report 108)*, August 2008, Recommendations 31-1 to 31-5, model UPP 11.

8 Mr Bruce Alston, ALRC, *Committee Hansard*, 16 August 2012, pp. 9-10.

9 See, for example, Australian Banking Association (ABA), *Submission 19*; Law Council of Australia (LCA), *Submission 4*; Foxtel, *Submission 24*; Australian Broadcasting Corporation (ABC), *Submission 5*.

10 Foxtel, *Submission 24*, p. 6.

- 2.8 The Law Council of Australia (LCA) acknowledged that APP 8 attempts to strike a balance between the protection of personal information and the convenient flow of information. However it suggests that, in this era of global trade, APP 8 errs too far on the side of cross border compliance at the expense of convenient flow of information and this may deter the growing use of cloud computing.¹¹
- 2.9 In this regard, some have suggested that there should be a defence to APP 8 available if the disclosing organisation has ‘taken reasonable steps’ to protect the information.¹²
- 2.10 Proposing a counter view, the Committee received many submissions suggesting APP 8 should include a much higher level of protection for personal information that is sent overseas.¹³
- 2.11 For example, the Australian Privacy Foundation (APF) is opposed to any defence to contravention.¹⁴ Similarly, the Office of the Privacy Commissioner, New South Wales (OPCNSW) suggests defences to contravention are inappropriate.¹⁵ The Office of the Australian Information Commissioner (OAIC) does not support defences to contraventions but considers that matters such as systems in place to prevent contraventions should be taken into account when determining the penalty.¹⁶
- 2.12 Some suggest individuals should be given prior knowledge before their personal information is sent overseas¹⁷ and consent should be required before it can be sent.¹⁸ The APF and OAIC further suggest that the exception in 8.2(e) should be removed.¹⁹
- 2.13 The Explanatory Memorandum to the Bill notes the attempt to strike a balance between data flow and privacy, stating that ‘the principle will aim to permit cross-border disclosure of personal information and ensure that

11 LCA, *Submission 4*, p. 10.

12 ABA, *Submission 19*, p. 11; Joint submission from Facebook, Google, Interactive Advertising Bureau (IAB) and Yahoo, *Submission 11*, p. 7.

13 See for example, APF, *Submission 30*; OAIC, *Submission 14*; Australian Communications Consumer Action Network (ACCAN), *Submission 26*.

14 APF, *Submission 30a*, p. 2; ACCAN, *Submission 26*, p. 10.

15 OPCNSW, *Submission 35*, p. 3.

16 OAIC, *Submission 14*, p. 4.

17 ACCAN, *Submission*, p. 9.

18 See ACCAN, *Submission 26*, p. 9; Macquarie Telecom, *Submission 10*, p. 2.

19 See APF, *Submission 30*; OAIC, *Submission 14*

any personal information disclosed is still treated in accordance with the Privacy Act.’²⁰

2.14 The Attorney-General’s Department confirms that it does not consider that APP 8.1 should include a general exception as this ‘would undermine the confidence of individuals in the protection of their personal information’²¹ and that ‘the exceptions in APP 8.2 have been carefully considered and the Government considers that they are justified’.²²

2.15 In relation to a defence for inadvertent disclosure, the Attorney-General’s Department stated:

The Government does not consider that an exception is necessary where the overseas recipient may have made an inadvertent disclosure of personal information. An inadvertent disclosure of personal information may have significant consequences for an individual. While a disclosure may be inadvertent, the fact the disclosure has occurred may indicate failures in the security systems or handling protocols of that personal information in the hands of the overseas recipient.²³

2.16 The Department considers an explicit defence is not required, as:

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.

It is not automatically the case that all possible or actual breaches of APP 8.1 will result in the imposition of a civil penalty. The decision to obtain a civil penalty order is at the discretion of the Commissioner, while the decision on whether a civil penalty should be imposed is at the discretion of the court.²⁴

2.17 In line with this, the Privacy Commissioner gave evidence that:

Where an organisation can demonstrate that it is taking these steps to try and limit the impact of the [data breach], whether they can demonstrate that, for example, they have put in the best standard or the highest standard of systems protection such as those

20 Privacy Amendment (Enhancing Privacy Protections) Bill 2012, *Explanatory Memorandum*, p. 83.

21 Attorney-General’s Department, *Submission 39*, p. 13.

22 Attorney-General’s Department, *Submission 39*, p. 13.

23 Attorney-General’s Department, *Submission 39*, p. 13.

24 Attorney-General’s Department, *Submission 39*, p. 13.

highlighted through international standards organisations, I certainly take that into account.²⁵

- 2.18 There have also been suggestions that it would be helpful if a list of countries that satisfy APP 8.2(a) was published.²⁶
- 2.19 At the Senate hearing, Mr Glenn, from the Attorney-General's Department gave evidence that:
- Certainly the ALRC recommended that the government publish a list of laws or binding schemes that would meet those criteria. The government response – this recommendation 31-6 – was to accept that. If this Bill is passed, the government will provide information about laws and binding schemes that it would consider are substantially similar to the APPs.²⁷
- 2.20 He noted, however, that there would still be an obligation on the disclosing party to ensure they were complying with the APPs in each set of particular circumstances.²⁸

Compliance with overseas laws

- 2.21 Some submissions suggest that the APPs do not allow for the fact that some Australian companies are required to comply with overseas laws as part of their business activities.²⁹ There is some concern that obligations in such overseas laws may conflict with the requirements of the APPs.
- 2.22 For example, the Australian Bankers Association notes that banks are subject to compliance with foreign laws such as the United States Foreign Accounts Tax Compliance Act 2010 (FACTA), which requires them to provide some personal information about United States nationals that hold Australian bank accounts. The Australian Bankers Association and the Australian Finance Conference suggest that the definition of 'Australian law' should include any applicable overseas law or government agreement binding on an organisation, which would allow organisations to comply with these overseas obligations.³⁰

25 Mr Timothy Pilgrim, OAIC, *Committee Hansard*, 16 August 2012, p. 7.

26 ABA, *Submission 19*, p. 11.

27 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August, p. 4.

28 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August, p. 4.

29 See, for example, Facebook, Google, IAB and Yahoo, *Submission 11*, p. 3; ABA, *Submission 19*, p. 5; Australian Finance Conference (AFC), *Submission 32*, p. 5.

30 ABA, *Submission 19*, p. 5; AFC, *Submission 32*, p. 5.

- 2.23 At the Senate hearing, the Attorney-General's Department suggested that the solution to this problem does not lie in reform of the *Privacy Act 1988* (Cth).³¹ It was suggested that FACTA requirements will not come into force until 2014, that they would also be inconsistent with the current requirements of the *Privacy Act 1988* (Cth) and that there are no changes implemented through the Privacy Amendment Bill that affect this.³²
- 2.24 The Department suggests that creating an exception similar to that proposed above is very broad and is problematic for sovereignty reasons.³³ There may be other mechanisms to prevent this conflict arising and discussions are being pursued between Australian Government agencies and the United States Internal Revenue Service to resolve this issue.³⁴
- 2.25 It is anticipated that the outcome of these discussions will be a negotiated solution to the issue before the FACTA obligations commence.³⁵

Direct marketing

- 2.26 The APP 7 is entitled 'prohibition on direct marketing'. APP 7.1 outlines a prohibition on direct marketing, and APPs 7.2 - 7.5 detail a number of exceptions to this prohibition.
- 2.27 In their submissions, the Australian Direct Marketing Association (ADMA), Foxtel, the LCA and Salmat all suggest that labelling these provisions as a 'prohibition' on direct marketing is misleading because, the provisions actually permit direct marketing in many circumstances.
- 2.28 The ADMA suggests that this title will create confusion for consumers and businesses and will result in marketing suppliers losing business when businesses believe direct marketing is now prohibited.³⁶ At the Senate

31 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August 2012, p. 8.

32 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August 2012, p. 8.

33 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August 2012, p. 8.

34 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August 2012, p. 8.

35 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August 2012, p. 8.

36 ADMA, *Submission 29*, p 5.

- hearing, Ms Jodie Sangster (ADMA) noted that \$15 billion is spent on direct marketing each year.³⁷
- 2.29 Foxtel suggests that consumer confusion will result in complaints about direct marketing where APP 7 is being complied with.³⁸
- 2.30 The LCA suggests APP 7 should be drafted in the style of APP 6, suggesting permission in certain situations and prohibition in all other situations.³⁹
- 2.31 Although the ALRC report suggested direct marketing be regulated in a discrete principle, their recommendation was not framed as a prohibition.⁴⁰
- 2.32 The ADMA recommends that the language and structure in the exposure draft be reinstated or alternatively, that similar drafting outlined by ADMA in their submission, be implemented.⁴¹
- 2.33 Foxtel suggests the section should be drafted to ensure clarity that there is an entitlement to market directly, subject to conditions.⁴²
- 2.34 The Attorney-General's Department suggests that this drafting approach was used 'to clearly identify the information-handling activity that breaches privacy'.⁴³
- 2.35 The Department also notes that the drafting approach was implemented as a result of comments and a recommendation made by the Senate Finance and Public Administration Legislation Committee that APP 7 be re-drafted to simplify terminology and clarify intent.⁴⁴ The Department suggests that the heading 'prohibition' was instated consistently with a clarity approach taken elsewhere in the Bill.⁴⁵

37 Ms Jodie Sangster, ADMA, *Senate Committee Hansard*, 10 August 2012, p. 35.

38 Foxtel, *Submission 24*.

39 LCA, *Submission 4*.

40 ALRC, *For your information: Australian Privacy Law and Practice (ALRC Report 108)*, August 2012, Recommendation 26-1.

41 ADMA, *Submission 29*, p. 6 and attachment A.

42 Foxtel, *Submission 24*, p. 5.

43 Attorney-General's Department, *Answer to Questions on Notice*, p. 1.

44 Attorney-General's Department, *Answer to Questions on Notice*, p. 1.

45 Attorney-General's Department, *Answer to Questions on Notice*, p. 1.

‘Opt out’ provisions for direct marketing

- 2.36 The APP 7.3(d) requires organisations to provide a prominent statement or to draw the individual’s attention to the option that an individual can request not to receive direct marketing in ‘each direct marketing communication’.
- 2.37 Foxtel, ADMA and Salmat’s submissions outline concern that such a requirement is not suited to all forms of direct marketing communication. In particular, for direct marketing in media such as Facebook and Twitter, which allow limited character space,⁴⁶ they suggest it is highly impractical to require that each communication include an opt out message.⁴⁷
- 2.38 The Attorney-General’s Department notes that these provisions will not cover all forms of direct marketing:
- 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.⁴⁸
- 2.39 The Department notes that the ‘opt out’ requirements are designed to operate flexibly so organisations can develop methods tailored to the specific form of advertising. It suggests that shorter messages inviting consumers to opt out through a link might be an option to consider.⁴⁹
- 2.40 Further, the Department notes that while these requirements will require organisations to adapt to new direct marketing rules, the rules will enhance the privacy protections of consumers.⁵⁰

46 Foxtel’s submission outlines in particular the impracticality of providing an opt out message within the constraints of the allocated 140 characters in a Twitter message at p. 5.

47 See Foxtel, *Submission 24*; ADMA, *Submission 29*; Salmat, *Submission 16*, p. 9.

48 Attorney-General’s Department, *Submission 39*, p. 2.

49 Attorney-General’s Department, *Submission 39*, p. 2.

50 Attorney-General’s Department, *Submission 39*, p. 2.

Committee comment

Defences to contravention

- 2.41 The Committee acknowledges the concerns raised by industry in relation to this matter. In addition, the Committee notes advice of the Attorney-General's Department and the Privacy Commissioner that reasonable steps taken by organisations will be taken into account in a determination at the OAIC and when the Privacy Commissioner makes a decision as to whether to seek a civil penalty order in relation to a breach. It notes that not all breaches will be dealt with by civil penalty.
- 2.42 The Committee accepts the Attorney-General's Department's concern that creating defences such as those proposed in some submissions may have a detrimental effect on the overall security of personal information in some circumstances.
- 2.43 Following due consideration, the Committee is of the view that the manner in which the provisions will function in practice will perhaps only be wholly understood once the regime is in operation. At this point, the Committee considers the correct balance has been achieved to ensure protection while permitting the flow of data required for effective business.
- 2.44 However, to safeguard the desired operation of the provisions, the Committee recommends that the prospect of introducing such a defence or exemption be re-evaluated in a review of the operation of the new privacy laws. This review should be conducted twelve months after the Act commences.

Compliance with overseas laws

- 2.45 The Committee acknowledges industry's concern regarding the conflict of certain overseas laws and the APPs.
- 2.46 However, based on advice from the Attorney-General's Department, the Committee concludes that this is not an issue specific to changes implemented through the Privacy Amendment Bill. Consequently, the Committee has not considered this issue in detail.
- 2.47 The Committee is pleased to note the Attorney-General's Department's intention to continue negotiations with stakeholders, with a view to identifying a method to prevent this conflict from arising.

Direct marketing

- 2.48 The Committee acknowledges industry's concerns that the characterisation of the direct marketing provision as a prohibition may have adverse effects for the direct marketing industry.
- 2.49 The Committee has not formed a view as to the degree of any adverse effect that may materialise but is satisfied this approach was taken following consultation and as a result of comments to the exposure draft of this Bill.
- 2.50 At this stage, the Committee considers that amendments to the drafting of these provisions are not required.

'Opt out' provisions for direct marketing

- 2.51 The Committee appreciates industry's concern about the requirements of the 'opt out' provisions for direct marketing. However, the Committee notes that APP 7 does not apply to all direct marketing, is intended to be flexible and can be fulfilled in a variety of ways.
- 2.52 The Committee is satisfied with the provisions as they stand, but suggests that their operation be evaluated in a review to be carried out twelve months after commencement of the Act.

Credit Reporting Provisions

- 3.1 The credit reporting provisions are contained in Schedule 2 of the Privacy Amendment Bill and will replace the current credit reporting system in Part IIIA of the *Privacy Act 1988* (Cth). The provisions regulate the handling and maintenance of certain kinds of personal information concerning consumer credit that is intended to be used wholly or primarily for domestic, family or household purposes.

The Australian link requirement

- 3.2 The Privacy Amendment Bill contains a specific rule to govern the cross-border disclosure of credit reporting information. A credit provider is restricted from disclosing credit eligibility information to overseas recipients that do not have an Australian link.¹ This requirement was not included in the 2011 exposure draft of the credit reporting provisions.
- 3.3 The Explanatory Memorandum states that ‘the term “Australian link” is used to define the entities that are subject to the operation of the Act’.²
- 3.4 The Australian link requirement aims to ensure Australian credit information does not leave the Australian credit information system and

1 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, clause 21G(3)(c)(ii).

2 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, *Explanatory Memorandum*, pp. 217-218.

that foreign credit information does not enter the Australian credit information system.³

3.5 The Committee received a significant number of submissions voicing concerns about the Australian link requirement in the credit reporting provisions.⁴ Many organisations are concerned that the Australian link restriction will inhibit legitimate business practices as information may not be able to be disclosed to an off-shore agent or related entity for legitimate business purposes.⁵

3.6 The Law Council of Australia (LCA) explains that:

...some 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. These services may comprise 'cloud' based technologies for data storage and backup, which may utilise storage in a variety of locations for the purposes of effective disaster recovery. In other cases, business processes (that may include automated credit decisioning or first line call centre support) may be hosted offshore by contracted service providers.

The off-shore 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.⁶

3.7 It appears that Australian organisations with such arrangements will be affected by the Australian link requirement.

3.8 Optus notes that the provisions will adversely affect companies that have off-shore call centres or data processing facilities.⁷

3.9 The Australia and New Zealand Banking Group Limited (ANZ) expresses concern that the provisions will mean an Australian-based organisation will not be able to transfer information to a wholly owned off-shore entity,

3 See Privacy Amendment (Enhancing Privacy Protections) Bill 2012, *Explanatory Memorandum*, p. 91; Mr Richard Glenn, Attorney-General's Department, *Committee Hansard*, 16 August, p. 17.

4 See, for example, Telstra, *Submission 15*; ABA, *Submission 19*, APF, *Submission 30* and the Insurance Council of Australia (ICA), *Submission 6*.

5 See, for example, ANZ, *Submission 22*, p. 4; LCA, *Submission 22*, p. 14.

6 LCA, *Submission 4*, p. 14.

7 Optus, *Submission 8*, p. 8.

even where the organisation takes steps to ensure the entity is subject to similar standards as the APPs.⁸

- 3.10 General Electric Capital notes that for companies that hold credit eligibility information and personal information, these will have to be segregated and managed under different disclosure regimes.⁹
- 3.11 The LCA suggests the Australian link requirement is artificial because if an Australian organisation has a 100 per cent held subsidiary performing outsourced services, the control that organisation holds over the information is the same, regardless of where the subsidiary is incorporated.¹⁰
- 3.12 The LCA suggests where the credit provider is an authorised deposit-taking institution for the purposes of the *Banking Act 1959* (Cth) and the manner in which the off-shore provider is being used is consistent with APRA's standards and is subject to APRA's supervision, the Australian link requirement should not apply.¹¹
- 3.13 Some submissions suggest that instead of the Australian link requirement, APP 8 should apply to credit eligibility information in the same way it applies to personal information¹² as there is no policy basis for restricting the disclosure of credit eligibility information to a greater degree than personal information.¹³
- 3.14 Alternatively, ANZ suggests that an exception to the Australian link requirement be developed for instances in which information is being disclosed for legitimate business purposes.¹⁴
- 3.15 In contrast, Communications Alliance suggests that Australian link requirement should be removed altogether.¹⁵
- 3.16 The Committee notes Mr Glenn from the Attorney-General's Department's comments at the Senate hearing, which acknowledged the issues and the ongoing discussions as to how the cross-border flow of credit information might best operate:
-

8 ANZ, *Submission 22*, p. 4.

9 General Electric Capital (GE), *Submission 7*, p. 3.

10 LCA, *Submission 4*, p. 14.

11 LCA, *Submission 4*, p. 14.

12 ANZ, *Submission 22*, p. 5; GE *Submission 7*, p. 3.

13 GE, *Submission 7*, p. 3.

14 ANZ, *Submission 22*, p. 5.

15 Communications Alliance, *Submission 9*, p. 11.

Certainly the Bill needs some improvements around the Australian link idea. We have heard from stakeholders that the proposed solution to deal with cross-border data flows in the credit context does not work with existing business models. So we are having some discussions with banking and finance stakeholder as to how to adjust that.¹⁶

3.17 The Attorney-General's Department notes that the Government accepted Australian Law Reform Commission (ALRC) recommendation 54-5 to exclude Australian reporting of personal information about foreign credit, and the disclosure of credit reporting information to foreign credit providers. The Department suggests that the off-shore processing of credit reporting information does not appear to have been considered by the ALRC.¹⁷

3.18 The Department's submission clarifies that there is no policy intention to prohibit the existing practices of credit providers in relation to their off-shore processing systems for credit reporting information.¹⁸

3.19 The Department explains that the insertion of the term 'Australian link' in section 5B of the *Privacy Act 1988* (Cth) (which includes a foreign organisation that holds information in Australia), combined with the permission for credit providers to disclose to a related body corporate, would allow off-shore processing of credit reporting data.¹⁹ However, it acknowledges that credit provider stakeholders suggest that this arrangement will not allow them to continue to undertake off-shore processing of that information.²⁰

3.20 The Department notes that:

On examining the exposure draft of the credit reporting provisions in the development of the Privacy Amendment Bill, it became clear that permitting broad cross-border disclosure of personal information from the credit reporting system under APP 8 would undermine the government's policy to exclude the reporting of personal information about foreign credit and the disclosure of credit reporting information to foreign credit providers.²¹

16 Mr Richard Glenn, Attorney-General's Department, *Senate Committee Hansard*, 21 August 2012, p. 3.

17 Attorney-General's Department, *Submission 39*, p. 5.

18 Attorney-General's Department, *Submission 39*, p. 5.

19 Attorney-General's Department, *Submission 39*, p. 6.

20 Attorney-General's Department, *Submission 39*, p. 6.

21 Attorney-General's Department, *Submission 39*, p. 6.

- 3.21 On this basis, the Department advises that it is currently considering options to address this issue. It notes that the preferred approach is to identify options that allow a specifically targeted disclosure to deal with off-shore process which would most likely impose obligations based on proposed APP 8.1 and proposed section 16C. This would ensure that the Australian credit provider remains accountable for the personal information sent to the overseas recipient. The Department advises that initial discussions suggest this approach may be acceptable to credit provider stakeholders.²²
- 3.22 The Committee was advised that the Department 'will continue to work with stakeholders to refine an approach that can be put to the Attorney-General for consideration.'²³

Repayment history data provisions

- 3.23 The Privacy Amendment Bill will allow personal information grouped under five new data sets to be collected and included on credit reports. The fifth new data set is repayment history data.
- 3.24 Some submissions outline their support for the inclusion of repayment history data as one of the new data sets.²⁴
- 3.25 However, some organisations have strong concerns about consumers' interests and the effect of the inclusion of repayment history data in the credit reporting system.²⁵
- 3.26 Notably, while the ALRC recommended that limited repayment history information should be included in the credit reporting system, it also recommends that this be accompanied by responsible lending obligations and other safeguards.²⁶

22 Attorney-General's Department, *Submission 39*, p. 6.

23 Attorney-General's Department, *Submission 39*, p. 6.

24 See, for example, ICA, *Submission 6*, p. 2; Communications Alliance, *Submission 9*, p. 10; Australian Retail Credit Association (ARCA), *Submission 12*, p. 13.

25 See, for example, APF, *submission 30*, Consumer Credit Legal Centre New South Wales (CCLC), *Submission 23*.

26 ALRC report, *For Your Information: Australian Privacy Law and Practice (ALRC report 108)*, August 2011, Recommendations 55-2 to 55-5.

- 3.27 The Explanatory Memorandum suggests that the repayment history data will lead to decreased levels of over indebtedness and lower credit default rates.²⁷ Other submissions also suggest that collection of repayment history data will improve the quality of consumer credit.²⁸
- 3.28 According to the Attorney-General's Department submission, the Government considers that more comprehensive credit reporting will allow a more robust assessment of credit risk. This could lead to lower credit default rates and is likely to improve competition in the credit market, eventually resulting in benefits to both individuals and the credit industry.²⁹
- 3.29 The Consumer Credit Legal Centre, New South Wales (CCLC) disputes this and claims there is no evidence to suggest that the inclusion of repayment history data will lead to these positive changes³⁰ and suggests that including repayment history data will not, in itself, lead to responsible lending.³¹
- 3.30 Instead, CCLC claims that the reverse may occur and there is the potential to justify the refusal of credit due to poor repayment history where the borrower otherwise has capacity to pay, or to allow credit to be granted where it wouldn't have been in other circumstances because of a good repayment history, or to offer differential pricing based on repayment history (risk-based pricing).³² These possible scenarios are unlikely to provide positive outcomes for consumers.³³
- 3.31 However, as noted in some submissions, lenders are already subject to various responsible lending obligations under the *National Consumer Credit Protection Act 2009 (Cth)*.³⁴
- 3.32 In addition, the Bill includes a number of consumer protections around repayment history information, such as a restrictive definition of 'repayment information' and strong restrictions on the collection, use and disclosure of repayment history information.³⁵

27 Privacy Amendment Bill 2012, *Explanatory Memorandum*, p. 3.

28 ICA, *Submission 6*, p. 3.

29 Attorney-General's Department, *Submission 39*, p. 7.

30 CCLC, *Submission 23*, p. 5.

31 CCLC, *Submission 23*, p. 5.

32 CCLC, *Submission 23*, p. 6.

33 CCLC, *Submission 23*, p. 6.

34 Abacus, *Submission 36*, p. 1; Experian, *Submission 27*, p. 7; ALRC, *Submission 33 attachment B*, pp. 2-3.

35 For more detail, see: Attorney-General's Department, *Submission 39*, p. 7.

- 3.33 The Committee also notes that the Government response to the ALRC recommendation 54-8 included an agreement that a review of the credit reporting provisions would be conducted within five years from the commencement of the Bill.³⁶
- 3.34 Most submissions to this inquiry raised concerns of industry regarding the effects of the Bill, however there were some additional issues raised by consumer advocates. These include the perceived reluctance of the Privacy Commissioner to make determinations, pre-screening for direct marketing purpose and the difficulty of removal of unfair/incorrect credit listings.
- 3.35 The Committee notes that many of these consumer advocate issues were interrogated in some detail at the Senate hearings and, consequently, the Committee has chosen not to examine further these issues.³⁷

Addresses stored on file

- 3.36 Veda's submission outlines its concern about the restriction on the number of addresses that can be held on a credit report. It suggests that the limit of an individual's current or last known address and two previous addresses, combined with changes which add restrictions on the internal use of that information, may result in many individuals becoming untraceable. This could potentially affect 2.4 million files.³⁸ As internal use is unregulated under the current regime, the additional information is used for data matching purposes.³⁹ Veda suggests that these restrictive changes will create potential for 'a highly mobile, highly transient segment of the population' to become untraceable.⁴⁰
- 3.37 Veda suggests that to remedy this problem the Bill should be amended to allow credit reports to include, for the purpose of record management, either the current plus two previous addresses or all addresses over the previous five years, whichever is the greater.⁴¹

36 Attorney-General's Department, *Submission 39*, p. 7.

37 See for example, the senate hearing transcripts.

38 Veda, *Submission 25, attachment B*, p. 1.

39 Mr Strassberg, Veda, *Senate Committee Hansard*, 10 August 2012, p. 28.

40 Mr Strassberg, Veda, *Senate Committee Hansard*, 10 August 2012, p. 28.

41 Veda, *Submission 25*, p. 3.

3.38 The Attorney-General's Department gave evidence that it does not consider that credit reporting bodies will lose trace of an individual if the individual moves more than twice in a five year period because the proposed definition of 'identification information' includes a range of other types of personal information.⁴²

3.39 The Attorney-General's Department notes that it:

...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.⁴³

Committee Comment

Australian link requirement

3.40 The Committee received a significant number of submissions on this issue and notes the difficulty in striking an appropriate balance between the protection of credit reporting information and the ability for industry to function reasonably. The Committee emphasises that this is critical issue.

3.41 The Committee notes that the Attorney-General's Department has already undertaken significant consultation with various organisations across many industries.

3.42 The Committee is pleased to note that the Attorney-General's Department intends to continue consultation with stakeholders. The Committee anticipates this process will lead to some resolution of the issues around the Australian link requirement.

3.43 At this point, the Committee is satisfied with the provisions as proposed in the Bill, particularly in light of continued consultation with industry which may refine aspects of the Bill's practical operation. However, given the complexity and seriousness of the issues, for both individuals and industry, the Committee acknowledges the critical importance of reviewing these provisions to assess their implementation and any unintended consequences. The Committee recommends that the cross border disclosure of credit reporting information is assessed in a review of

42 Attorney-General's Department, *Answers to Questions on Notice*, p. 8.

43 Attorney-General's Department, *Answers to Questions on Notice*, p. 9.

the operation of the new privacy laws. This review should be conducted twelve months after the Act commences.

Repayment history provisions

- 3.44 The Committee notes concerns raised regarding the effect of the inclusion of repayment history provisions. However, responsible lending obligations already exist and, as per the recommendation of ALRC, consumer protections are included in the Bill.
- 3.45 The Committee supports the Government's commitment to review the credit reporting provisions within five years of commencement.
- 3.46 The Committee is satisfied that the provisions as currently drafted are reasonable and balanced, and an appropriate review of their operations has already been agreed to.

Addresses stored on file

- 3.47 The Committee notes the concern raised regarding this issue but is not convinced that it will result in many individuals becoming untraceable as a consequence. Other types of personal information may still be stored and the Committee does not consider the changes to be overly restrictive or detrimental to industry.

Further issues

- 4.1 A number of additional issues regarding elements of the Privacy Amendment Bill were raised in submissions. Some of these issues are addressed in this chapter.

De-identified data

- 4.2 Proposed section 20M(1) of the Privacy Amendment Bill outlines a prohibition on credit reporting bodies using or disclosing de-identified credit reporting information. Proposed section 20M(2) then outlines an exception that such de-identified data may be disclosed for the purpose of conducting research in relation to the assessment of the credit worthiness of individuals if the credit reporting body complies with certain rules.
- 4.3 De-identified data was not previously regulated by Australian privacy laws and the Australian Law Reform Commission (ALRC) report did not recommend that de-identified data be regulated.
- 4.4 The Committee received evidence that no other modern economy regulates de-identified data.¹ This is likely because, once de-identified, the information is no longer personal information and therefore does not fall within the remit of privacy laws.²

1 Veda, *Submission 25*, p. 1; Professor Les McCrimmon, *Senate Committee Hansard*, 10 August 2012, p. 24.

2 See Professor Les McCrimmon, *Senate Committee Hansard*, 10 August 2012, p. 24; ARCA, *Submission 12*, p. 7; ANZ, *Submission 22*, p. 8.

- 4.5 De-identified credit reporting data is used to compile studies around credit risk and economic hardship in Australia.³ It is also used for internal credit modelling and portfolio management, which Australia and New Zealand Banking Group Ltd suggests assists in the assessment of credit applications and helps banks to lend responsibly.⁴
- 4.6 Veda notes that de-identified data is:
- ...critical for creating data series, accurate statistical modelling and developing insights into historic trends. It helps ensure the accuracy of credit risk models and the insights it can contribute are also provided to key financial pillars such as the Reserve Bank.⁵
- 4.7 Several submissions suggest the restrictions on the use of de-identified data in this Bill are unnecessary and may lead to unjustified restrictions on the research and development work undertaken with this data.⁶
- 4.8 Some submissions recommend that section 20M be removed from the Bill in its entirety⁷ or that the majority of the section be deleted.⁸ Some also suggest that a better approach would be to create a penalty for anyone found to have re-identified data.⁹ In addition, it is suggested that if data is re-identified, then it would then be personal information and any misuse of that information would be regulated by the Australian Privacy Principles (APPs). This should ensure sufficient protection.¹⁰
- 4.9 The Explanatory Memorandum states that the purpose of regulating de-identified credit reporting information is to 'clarify that such information can be used or disclosed in specified circumstances'¹¹ but notes concern 'about the effectiveness of methods used to de-identify

3 Veda, *Submission 25*, p. 4.

4 ANZ, *Submission 22*, p. 8.

5 Veda, *Submission 25*, p. 1.

6 ARCA, *Submission 12*, p. 7; Veda, *Submission 25*, p. 5; ANZ, *Submission 22*, p. 8. See also Professor Les McCrimmon's, *Senate Committee Hansard*, 10 August 2012, p. 24. Veda's submission lists a number of important studies that were conducted with depersonalised data.

7 Australian Retail Credit Association, *Submission 12*, p. 7; ANZ, *Submission 22*, p. 8; Australian Finance Council, *Submission 32*, p. 10.

8 Veda, *Submission 25*, p. 3.

9 Australian Retail Credit Association, *Submission 12*, p. 7. See also Professor Les McCrimmon's, *Senate Committee Hansard*, 10 August 2012, p. 24..

10 Veda, *Submission 25*, p. 3.

11 Privacy Amendment (Enhanced Privacy Protections) Bill 2012, *Explanatory Memorandum*, p. 144.

personal information and the risks of that information subsequently being linked again to individuals in a way that allows them to be identified.’¹²

- 4.10 The Australian Privacy Foundation’s submission echoes this concern. It draws the Committee’s attention to the ‘increasingly contentious’ issue of whether the de-identification of data can really be guaranteed,¹³ and notes that re-identification technologies are growing rapidly.¹⁴
- 4.11 Veda submits that these risks relate to health data and not credit reporting data,¹⁵ and that re-identification is a problem that has taken place in the United States where more comprehensive, large-scale, public data sources are readily available.¹⁶
- 4.12 Proposed section 20M’s purpose is to ensure that the Privacy Commissioner has the power to issue appropriate guidelines to deal with the way de-identified data is used.¹⁷
- 4.13 The Attorney-General’s Department noted that their advice from credit reporting agencies is that those agencies de-identify information prior to using it in studies. However the Attorney-General’s Department states that it is unclear how this is done.¹⁸ Given the uncertainty around this, the Government’s view when drafting the Bill was that the proposed approach to de-identified data is the optimal one.¹⁹

Commencement period

- 4.14 Several submissions suggest that the Privacy Amendment Bill’s proposed nine month period between Royal Assent and commencement date is unreasonably short.²⁰
- 4.15 The Australian Bankers Association (ABA) notes:

12 Privacy Amendment (Enhanced Privacy Protections) Bill 2012, *Explanatory Memorandum*, p. 144.

13 APF, *Supplementary Submission 30a*, p. 3.

14 APF, *Supplementary Submission 30a*, p. 3.

15 Veda, *Submission 25*, p. 7; Professor Les McCrimmon’s, *Senate Committee Hansard*, 10 August 2012, p. 24.

16 Veda, *Submission 25*, p. 4.

17 Attorney-General’s Department, *Submission 39*, p. 9.

18 Attorney-General’s Department, *Submission 39*, p. 9.

19 Attorney-General’s Department, *Submission 39*, p. 9.

20 ABA, *Submission 19*, p. 3; AFC, *Submission 32*, p. 4; ARCA, *Submission 12*, pp. 7-9.

The credit reporting reforms will require individual banks to develop their own internal compliance arrangements together with ensuring that their IT systems can interface with external credit reporting bureaux systems. Further, credit reporting bureaux will have to implement their own compliance arrangements.²¹

- 4.16 The Australian Retail Credit Association (ARCA) suggests a four step process ensuring the Credit Reporting code (CR code) is finalised before the commencement date is set down²² because some of ARCA's members will only be able to undertake the full implementation process once the Office of the Australian Information Commissioner (OAIC) has approved the CR code.²³
- 4.17 The ABA suggests a commencement period of 15 to 18 months would be adequate.²⁴
- 4.18 The Australian Finance Conference suggested that rather than adopting a fixed date for commencement, an approach that enables a date to be determined by the Minister should be included in the Bill.²⁵
- 4.19 The Attorney-General's Department notes that the standard three month commencement period has already been extended to nine months. This was decided on the understanding that this would be a sufficient period leading to registration of the CR code, on advice from the OAIC and relying on precedent in terms of commencement periods of other regulatory changes.²⁶
- 4.20 The Department notes:

The commencement period should provide sufficient time for the development, approval and registration of the CR code, 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).

The Department does not consider that commencement should be at the discretion of the Attorney-General, nor does the Department

21 ABA, *Submission 19*, p. 3.

22 ARCA, *Submission 12*, pp. 7-9.

23 Mr Damian Paull, ARCA, *Senate Committee Hansard*, 10 August 2012, p. 14.

24 ABA, *Submission 19*, p. 4.

25 AFC, *Submission 32*, p. 4.

26 Attorney-General's Department, *Submission 39*, p. 10.

consider that the commencement should be contingent on the registration of the CR code as this does not ensure certainty.²⁷

- 4.21 The Department has stated that it will be considering stakeholder views on extending the proposed nine month commencement period in proposing options for consideration by the Attorney-General.²⁸

Complexity

- 4.22 The Committee received many submissions suggesting that various parts of the Privacy Amendment Bill are complex and confusing²⁹ which may make the new privacy regime difficult to use and apply.³⁰
- 4.23 The ALRC noted the complexity of the privacy regime in its report and make a multitude of recommendations that the Privacy Commissioner publish guidance and educational materials on a variety of topics.³¹
- 4.24 There have been further suggestions that educational materials should be developed to render this complex legislation more accessible to the public.³²
- 4.25 The Attorney-General's Department states that it is not considering any comprehensive redrafting or restructuring of the Bill and that it expects that the structure of some of the reforms that may not be currently discernible will become apparent when the amendments are incorporated and the Privacy Act is a single document.³³
- 4.26 The Department also notes that in relation to the credit reporting provisions, increased complexity may be the result of the significant increase in complexity and scale since the credit reporting system's introduction twenty years ago.³⁴
- 4.27 The Department acknowledges the recommendations the ALRC directed to the OAIC on the provision of guidance and educational materials and

27 Attorney-General's Department, *Submission 39*, p. 10.

28 Attorney-General's Department, *Submission 39*, p. 11.

29 See, for example, CCLC, *Submission 23*, p. 4; APF, *Submission 30*; OPCNSW, *Submission 35*, p. 4.

30 CCLC, *Submission 23*, p. 4.

31 See, for example, ALRC, *For your Information: Australian Privacy Law and Practice (ALRC Report 108)*, August 2008, Recommendation 6-2, 10-2, 10-3, 68-4, 70-3.

32 See, for example, the comments of Ms Ganopolsky (LCA) and Ms Miller (Law Institute of Victoria), Senate Committee Hansard, p. 47.

33 Attorney-General's Department, *Submission 39*, p. 4.

34 Attorney-General's Department, *Submission 39*, p. 4.

notes that the Government accepted those recommendations in principle.³⁵ The Department supports the development of educational materials in relation to the new privacy regime but suggests that it is a matter for the OAIC.³⁶

Committee comment

De-identified data

- 4.28 The Committee acknowledges industry's concern that important studies may be obstructed through the regulation of de-identified data. In addition, the Committee appreciates concerns about the risk of re-identification of data.
- 4.29 The Committee has not formed a view as to whether the risk of re-identification of data is so severe that the regulation of de-identified data is justified, given lack of precedent in other modern economies.
- 4.30 The Committee acknowledges the importance of the studies undertaken with such data and while it suggests the Bill proceed in its current form, it suggests that the operation of section 20M be evaluated in a review to be conducted twelve months after commencement of the Act.

Commencement period

- 4.31 The Committee is concerned by the issues raised in relation to the commencement date. The Committee has not formed a specific view as to the length of time industry genuinely requires to implement internal systems required to comply with the new credit reporting system. However, the Committee considers that the CR code should be developed and approved by the Privacy Commissioner as soon as possible, to allow industry the greatest time possible to implement required systems.
- 4.32 The Committee notes the Attorney-General's Department continue to consult stakeholders and propose options to the Attorney-General. Consequently, the Committee anticipates that the issue may be resolved to a large degree through this consultative process.

35 Attorney-General's Department, *Submission 39*, p. 4.

36 Attorney-General's Department, *Submission 39*, p. 4.

Complexity

- 4.33 The Committee appreciates that updating Australia's privacy laws is a complex task that requires detailed provisions. It acknowledges that these reforms were informed by a comprehensive ALRC inquiry and significant scrutiny and time have gone into their development. In addition, the Committee notes that one of the aims of the reforms was to reduce complexity.
- 4.34 Accordingly, the Committee is concerned by the number of submissions that suggest significant confusion around the new provisions. The Committee is concerned whether the public will be able to easily comprehend new privacy rights and whether industry will comprehend the obligations placed on them.
- 4.35 The Committee notes that the Government has accepted in principle the recommendation of the ALRC to develop educational materials. The Committee considers this is essential given the complexity and seriousness of these provisions.
- 4.36 The Committee notes that no agency has indicated to the Committee that they are developing such material, or that they consider themselves responsible for the development of such material. This is of grave concern to the Committee and the Committee recommends that the Attorney General ensure that comprehensive material setting out new privacy obligations and protection is available prior to the commencement of the Act.

Concluding remarks

- 4.37 Given the seriousness of privacy concerns and that Australian privacy laws have not been updated for twenty years, the Committee recognises the importance of the enhanced privacy protections proposed in this Bill.
- 4.38 In examining the Bill, the Committee has looked to ensure that an appropriate balance between privacy protection and the convenient flow of data has been achieved. Given the complexity of issues and the global nature of business, there are many elements to the privacy regime proposed and there remain many areas of concern to industry and consumer advocates.
- 4.39 The Committee recognises that considerable consultation has gone on prior to the introduction of this Bill to the House, and that many of the

provisions proposed are the enactment of recommendations made in the ALRC review. In addition, the Committee notes that the Attorney-General's Department is continuing to consult with stakeholders to resolve a number of the implementation details around this Bill and to discuss further possible consequences of the Bill.

4.40 However, given the degree of concerns and that Departmental consultations are continuing with the purpose of potentially advising the Attorney-General of options, the Committee expresses its disappointment that the House and indeed this Committee is asked to consider the Bill at this stage.

4.41 On balance the Committee has determined to recommend that the Privacy Amendment Bill be passed by the House of Representatives. The Committee adopts this position because it considers that there is a critical need to increase consumer privacy protections.

Recommendation 1

4.42 **The Committee recommends that the House of Representatives pass the Privacy Amendment (Enhancing Privacy Protections) Bill 2012.**

4.43 While recommending that this Bill should be passed (subject to the outcome of continuing consultations with stakeholders), the Committee further recommends that the Attorney-General conduct a review of the functioning of the new privacy regime twelve months after the Bill commences. This review should address a number of issues that have been raised in this inquiry.

Recommendation 2

4.44 The Committee recommends that the Attorney-General agree to conduct a review of the Privacy Amendment (Enhancing Privacy Protections) Bill 2012 twelve months after the commencement of the Act, addressing the following issues:

- Defence to contravention of APP 8
- Conflicting overseas laws
- Direct marketing and opt out provisions for direct marketing
- De-identified data provisions
- The system regulating/preventing credit reporting information overseas (the Australian link requirement), and
- The effect of the repayment history provisions on addresses stored on file.

4.45 The Committee is concerned that suitable educational and explanatory material will need to be developed prior to the commencement of the Act to ensure that individuals understand their new privacy rights, and that industry are fully aware of their obligations.

4.46 During the inquiry, it was not clear that any agency was to assume responsibility for the development and distribution of such material. Failure to ensure all parties are aware of and fully understand their obligations and protections would be a grave oversight in the implementation of this new privacy regime.

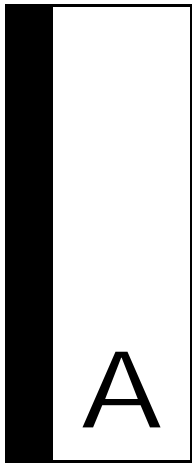
4.47 Accordingly, the Committee recommends that the Attorney-General ensure that suitable educational material is developed and distributed prior to the commencement of the Act.

Recommendation 3

- 4.48 **The Committee recommends that the Attorney-General ensure that comprehensive educational material on the new privacy protections and obligations is available prior to commencement of the Act.**

Graham Perrett MP

Chair



Appendix A – List of Submissions

- 1 Ms Julie Edwards
- 2 Consumer Action Law Centre
- 3 Mr Kevin Cox
- 4 Law Council of Australia
- 5 Australian Broadcasting Corporation
- 6 Insurance Council of Australia
- 7 GE Capital
- 8 Optus
- 9 Communications Alliance Ltd
- 10 Macquarie Telecom
- 11 Google Australia & New Zealand, Facebook Australia & New Zealand, IAB Australia and Yahoo!7
- 12 Australasian Retail Credit Association
- 13 Microsoft Australia
- 14 Office of the Australian Information Commissioner
- 14 a Office of the Australian Information Commissioner
Supplementary Submission
- 15 Telstra
- 16 Salmat
- 17 Australian Information Industry Association
- 18 National Relay Service

- 19 Australian Bankers' Association
- 19a Confidential
Supplementary Submission
- 20 Castan Centre for Human Rights Law
- 21 Financial Services Council
- 22 ANZ
- 23 Consumer Credit Legal Centre Inc. New South Wales
- 24 Foxtel
- 25 VEDA
- 26 Australian Communications Consumer Action Network
- 27 Experian Australia Credit Services Pty Ltd
- 28 Liberty Victoria
- 29 Australian Direct Marketing Association
- 29a Australian Direct Marketing Association
Supplementary Submission
- 30 Australian Privacy Foundation
- 30a Australian Privacy Foundation
Supplementary Submission
- 31 Yahoo!7
- 32 Australian Finance Conference
- 32a Australian Finance Conference
Supplementary Submission
- 33 Australian Law Reform Commission
- 33a Australian Law Reform Commission
Supplementary Submission
- 34 Office of the Victorian Privacy Commissioner
- 35 Information and Privacy Commission

- 36 Abacus - Australian Mutuals
- 37 Telecommunications Industry Ombudsman
- 38 NSW Department - Attorney General and Justice
- 39 Attorney-General's Department



Appendix B – List of Witnesses Appearing at Public Hearing

Thursday, 16 August 2012 - Canberra

Attorney-General's Department

Mr Sam Ahlin, Principal Legal Officer

Mr Richard Glenn, Assistant Secretary, Business and Information Law Branch

Mr Colin Minihan, Principal Legal Officer, Business and Information Law Branch

Australian Law Reform Commission

Mr Bruce Alston, Principal Legal Officer

Professor Rosalind Croucher, President

Law Council of Australia

Ms Olga Ganopolsky, Chair, Business Law Section Privacy Committee

Office of the Australian Information Commissioner

Ms Angelene Falk, Director Policy

Mr Timothy Pilgrim, Australian Privacy Commissioner