Australian Government

Office of the Australian Information Commissioner

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Submission to the House of Representatives Standing Committee on Social Policy and Legal Affairs

24 July 2012

Timothy Pilgrim

Privacy Commissioner

Table of Contents

Executive summary

i. The Office of the Australian Information Commissioner (OAIC) welcomes the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (the Bill) and supports the Government's commitment to create a 'clear and simple framework for privacy rights and obligations',[1] introduce a more comprehensive credit reporting system with improved privacy protections and introduce a range of new functions and powers for the Commissioner. The OAIC has considered the Bill in light of the objectives underpinning the need for reform, in particular, that privacy rights and obligations are easy to understand and apply, and that existing privacy protections are maintained, not diminished.

ii. While the OAIC supports the Bill and the enhancements to current privacy regulation it proposes, the OAIC's comments in this submission focus on the parts of the Bill where there remains further scope for the simplification, clarification and enhancement of the privacy framework.

Key Recommendations

iii. To give effect to the Government's commitment to create a clear and simple framework for privacy rights and obligations, and to the other objectives of the reform,[2] the OAIC has made recommendations where it considers that the provisions of the Bill could be further simplified, clarified or enhanced. These recommendations have been grouped under five categories:

A. General issues in the proposed Australian Privacy Principles (APPs)

B. Specific issues in the proposed APPs

C. General Issues in the proposed credit reporting provisions

D. Specific Issues in the proposed credit reporting provisions

E. Specific issues on which the House of Representatives Standing Committee on Social Policy and Legal Affairs invited comment

A. General issues in the APPs

iv. Where an exception to the obligations imposed by the APPs is required to permit specific information handling activities of certain agencies, the OAIC recommends that the exception be addressed in the agencies' enabling legislation or under the Commissioner's power to make a Public Interest Determination (PID) (see paragraphs 12-18).

[1] The Australian Government 2009, *Enhancing National Privacy Protection, Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (Government first stage response), p 6, available at http://www.ag.gov.au/Privacy/Pages/Privacy-Reforms.aspx.

[2] For a summary of the objectives of the reforms see the former Office of the Privacy Commissioner (OPC) 2010, *Submission to the Senate Finance and Public Administration Committee on the Australian Privacy Principles Exposure Draft and Companion Guide* (APP Submission), para 9, available at http://www.privacy.gov.au/materials/types/submissions/view/7125.

v. In line with the recommendation in clause iv above, the OAIC recommends removing the exceptions in Permitted General Situation (PGS) 6 (relating to diplomatic or consular functions and activities) and PGS 7 (relating to activities of the Defence Force). If those exceptions are retained, the OAIC recommends that they be subject to rules made by the Commissioner (see paragraphs 19-25).

vi. In line with the recommendation in clause iv above, the OAIC recommends removing the Immigration Department from the definition of 'enforcement body' in s 6 of the *Privacy Act 1988* (Cth) (Privacy Act) (as amended by items 16-19 of Schedule 1 of the Bill) (see paragraphs 26-28).

vii. The Explanatory Memorandum to the Bill (Explanatory Memorandum) clarifies that the term 'necessary' implies an objective test and that the term 'reasonably necessary' is intended to provide a comparable level of protection. For simplicity, clarity and certainty, the OAIC therefore recommends replacing the phrase 'reasonably necessary' with the phrase 'necessary' throughout the APPs (see paragraphs 29-33).

viii. The OAIC considers that in some instances, the use of the subjective standard 'believes' to determine when certain activities are excepted from the obligations imposed by the APPs, results in the threshold being set too low. Subject to the recommendation at clause v above, the OAIC suggests amending the wording of PGS 6, PGS 7 and APP 3.4(d) by removing the words 'reasonably believes' and instead relying on the objective standard of 'necessary' (in line with the recommendation at clause vii above) (see paragraphs 34-40).

ix. In keeping with the Government's commitment to create a clear and simple framework for privacy rights and obligations through the creation of a single set of high-level principles – the APPs – the OAIC considers that the different standards for agencies and organisations in APP 3 ('collection of solicited personal information') are unnecessary. The OAIC recommends removing the words 'directly related to' from APPs 3.1, 3.3(a)(i) and 3.4(d) to ensure that consistent information handling practices apply to both agencies and organisations (see paragraphs 41-45).

x. The Explanatory Memorandum clarifies that the reference to the collection of personal information 'in Australia' in s 5B(3)(c) of the Privacy Act (as amended by item 7 in Schedule 4 of the Bill) includes the collection from an individual that is physically within Australia by an overseas entity. Given the importance of s 5B(3) in determining the entities that are subject to the Privacy Act, the OAIC recommends making this meaning explicit in the Bill (see paragraphs 46-49).

B. Specific issues in the APPs

xi. Noting that sensitive information should be accorded higher standards of protection; that the Bill amends the definition of non-profit organisations (NPOs) to cover a broader class of organisations; and the OAIC's view that a requirement that information be 'related to' an NPO's activities sets a lower threshold than a requirement that information be 'reasonably necessary' for the activity, the OAIC recommends amending the exception to the collection of sensitive information by

NPOs in APP 3.4(e)(i) to require that the information be 'necessary for' the NPO's activities in line with recommendation at clause vii above (see paragraphs 50-54).

xii. The Explanatory Memorandum clarifies that the obligation on APP entities to collect personal information by 'fair means' in APP 3.5(c) would include a requirement not to use means of collection that are unreasonably intrusive. The OAIC recommends that the Bill be amended to make this obligation explicit. This obligation is important in order to ensure that personal information is collected in a way that is not unreasonably intrusive and takes account of the cultural sensitivities of different communities and groups within Australia (see paragraphs 55-57).

xiii. The OAIC recommends removing the exception relating to the disclosure of biometric information by an agency to an enforcement body in APP 6.3. The exceptions in APP 6.2 already permit agencies to share sensitive information without consent in a wide range of circumstances. These exceptions and the ability to include appropriate authorisations in agencies' enabling legislation or the ability of the Commissioner to make a PID, are sufficient and more appropriate mechanisms to permit such disclosures (see paragraphs 58-62).

xiv. If, contrary to the recommendation at clause xiii above, the exception to disclosure in APP 6.3 is retained, the OAIC recommends replacing the reference to 'guidelines' in APP 6.3(d) with 'rules' (see paragraph 63).

xv. The OAIC recommends removing the exception in APP 8.2(e) that allows agencies to disclose personal information overseas in accordance with international agreements relating to information sharing without complying with APP 8.1 and the accountability requirements in clause 16C of the Bill. To ensure that agencies' information handling activities are subject to sufficient scrutiny, the OAIC recommends that disclosure should only be excepted from the requirements of APP 8.1 and clause 16C if obligations under such agreements are incorporated into domestic law. Alternatively, those disclosures may be the subject of a PID made by the Commissioner (see paragraphs 64-69).

C. General issues in the credit reporting provisions

xvi. To ensure that the credit reporting provisions are readily accessible and easily understood, and to achieve consistency with the proposed approach of placing the APPs in a Schedule to the Privacy Act, the OAIC recommends including the credit reporting provisions in Part IIIA of the Privacy Act (as amended by Schedule 2 of the Bill) in a Schedule to the Act (see paragraphs 70-72).

xvii. The OAIC recommends that, in order to give effect to the Government's intention to exclude foreign credit and foreign credit providers, they be explicitly excluded by specific provisions in the Bill. The OAIC considers that such an approach would create greater clarity and certainty, and more effectively achieve the Government's intention (see paragraphs 73-79).

D. Specific Issues in the credit reporting provisions

xviii. The OAIC recommends that the operation of the correction process, in circumstances where the credit reporting body (CRB) or credit provider does not hold the item of personal information the individual seeks to have corrected, be clarified to ensure that the correction and notification obligations in the Bill are clear, appropriate and comprehensive (see paragraphs 80-84).

E. Specific Issues on which the House of Representatives Standing Committee on Social Policy and Legal Affairs invited comment

xix. The OAIC does not support the availability of defences to contraventions of the Privacy Act (as amended by the Bill) for inadvertent disclosures. Rather, the OAIC considers that the circumstances of the disclosure, including whether the entity has taken reasonable steps to incorporate appropriate security protections into its systems, should be taken into account in determining the form and/or amount of any remedy or penalty (see paragraphs 86-88).

xx. The OAIC considers that if the handling of de-identified credit related information for research purposes is regulated under the Bill, it is important that such regulation is consistent with other areas of the Privacy Act, and gives appropriate consideration to the types of information involved, its current usage, and community sensitivities and expectations (see paragraphs 89-92).

Office of the Australian Information Commissioner

1. The Office of the Australian Information Commissioner (the OAIC) was established by the *Australian Information Commissioner Act 2010* (the AIC Act) and commenced operation on 1 November 2010. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner (the Commissioner). The former Office of the Privacy Commissioner (OPC) was integrated into the OAIC on 1 November 2010.
2. The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.
3. The Commissioners of the OAIC share two broad functions:
   - the FOI functions, set out in s 8 of the AIC Act – providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982*
   - the privacy functions, set out in s 9 of the AIC Act – protecting the privacy of individuals in accordance with the *Privacy Act 1988* (the Privacy Act) and other legislation.
4. The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

Introduction

5. The OAIC welcomes the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (the Bill), and the enhancements to current privacy regulation contained in the Privacy Act it proposes. The OAIC supports the Government's commitment to create a 'clear and simple framework for privacy rights and obligations',[3] introduce a more comprehensive credit reporting system with improved privacy protections and introduce of a range of new functions and powers for the Commissioner, consistent with the Government's first stage response. The new functions and powers will assist in addressing serious and systemic interferences with individuals' privacy, and provide a clear message to entities of the need to take privacy seriously.
6. The OAIC supports the simplification of the Privacy Act through the consolidation of the National Privacy Principles (NPPs) and the Information Privacy Principles (IPPs) into a single set of high-level principles – the Australian Privacy Principles (APPs). In its submission to the Senate Finance and Public Administration Committee (Senate Committee) on the Exposure Draft of the APPs (APP Submission), the OPC

[3] Government first stage response, p 6.

emphasised the importance of considering the APPs in light of whether they achieve the objectives underpinning the need for reform.[4] That submission also suggested a number of improvements to the APPs to better achieve those objectives. The OAIC notes, in particular, the need to ensure that privacy rights and obligations are simplified and therefore easy to understand and apply, and that existing privacy protections are maintained,[5] not diminished.[6]

7. The OAIC has considered the Bill in the context of its role as the agency that will investigate potential breaches of the Privacy Act, advise individuals of their privacy rights and educate entities on their new obligations. The OAIC supports the Bill, including the creation of the APPs, as an important step towards achieving the reform objectives, but considers that the effectiveness of the Bill in achieving these objectives could be further enhanced. The OAIC's comments below relate to those parts of the Bill where there remains an opportunity for simplification, clarification or enhancement of privacy regulation.

Background

8. The introduction of the Bill into Parliament on 23 May 2012 was a significant milestone in a long process of privacy law reform, in which the OAIC has been actively involved.

- In January 2006 the ALRC received a reference from the then Australian Government to undertake a review of the Privacy Act. The ALRC's review of privacy from 2006 to 2008 included the release of Issues Papers 31 and 32, Discussion Paper 72, and extensive consultation, culminating in the release of Report 108, *For Your Information, Australian Privacy Law and Practice* in August 2008 (ALRC Report 108).[7]
- In October 2009 the Government announced its first stage response to ALRC Report 108, covering 197 of the 295 recommendations.[8] The Government has indicated that it will respond to the remaining recommendations in the ALRC Report 108 at a later stage.[9]
- The Australian Government released two exposure drafts for consideration by the Senate Committee: Exposure Draft legislation for the APPs in June 2010 (Exposure Draft APPs) and the Exposure Draft credit reporting provisions in February 2011 (Exposure Draft credit reporting provisions).

[4] Those objectives are set out in the APP Submission, para 9.
[5] Government first stage response (2009), pp 11 and 13.
[6] Australian Law Reform Commission (ALRC) 2008, *For Your Information, Australian Privacy Law and Practice*, Report No. 108 (ALRC Report 108), recommendation 5-2, available at http://www.alrc.gov.au/publications/report-108; accepted in the Government first stage response, p 22.
[7] ALRC 2006, *Issues Paper 31: Review of Privacy,* available at http://www.alrc.gov.au/ip-31; ALRC 2006, *Issues Paper 32: Review of Privacy-Credit Reporting Provisions,* available at http://www.alrc.gov.au/ip-32; ALRC 2007, *Discussion Paper 72: Review of Australian Privacy,* available at http://www.alrc.gov.au/dp-72; ALRC Report 108.
[8] Government first stage response, p 9.
[9] Government first stage response, p 9.

- In August 2010, the OPC made a submission to the Senate Committee on the Exposure Draft APPs.[10] In March 2011, the OAIC made a submission to the Senate Committee on the Exposure Draft credit reporting provisions (Credit Reporting Submission).[11]
- The Senate Committee released its report on the Exposure Draft APPs in June 2011 (APP Report) and its report on the draft credit reporting provisions in October 2011 (Credit Reporting Provisions Report), each of which made a range of recommendations.[12]
- In May 2012, the Government responded to the Senate Committee reports (Government Senate Committee APP Response and Government Senate Committee Credit Reporting Response).[13]
- Following its introduction into Parliament on 23 May 2012, the Bill was referred to the House of Representatives Standing Committee on Social Policy and Legal Affairs on 24 May 2012. Subsequently, on 19 June 2012, the Bill was referred the Senate Legal and Constitutional Affairs Committee.

The Bill

9. The Bill amends the Privacy Act to implement the Government's first stage response to the ALRC Report 108. Specifically, the Explanatory Memorandum to the Bill (Explanatory Memorandum) explains that the Bill amends the Privacy Act to:

    - consolidate the NPPs and the IPPs into a single set of high-level principles – the APPs
    - introduce a more comprehensive credit reporting system with improved privacy protections
    - introduce new provisions on privacy codes and the credit reporting code (called the CR code), including powers for the Commissioner to develop and register

[10] OPC 2010, *Submission to the Senate Finance and Public Administration Committee on the Australian Privacy Principles Exposure Draft and Companion Guide*.
[11] Office of the Australian Information Commissioner (OAIC) 2011, *Submission to the Senate Finance and Public Administration Committee on the Credit Reporting Exposure Draft and Companion Guide* (Credit Reporting Submission), available at http://www.oaic.gov.au/publications/submissions.html#2011.
[12] Senate Finance and Public Administration Committee 2011, *Exposure Drafts of Australian Privacy Amendment Legislation Report Part 1 – Australian Privacy Principles* (APP Report), available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/index.htm; Senate Finance and Public Administration Committee 2011, *Exposure Drafts of Australian Privacy Amendment Legislation Report Part 2 – Credit Reporting* (Credit Reporting Provisions Report), available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/index.htm.
[13] The Australian Government 2012, *Government Response to the Senate Finance and Public Administration Legislation Committee Report: Exposure Drafts of Australian Privacy Amendment Legislation: Part 1 – Australian Privacy Principles* (Government Senate Committee APP Response), available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/index.htm.

codes in the public interest that are binding on specified agencies and organisations

- clarify the existing functions and powers of the Commissioner, and introduce new functions and powers that will assist in promoting compliance with privacy obligations.[14]

10. The substantive elements of the reforms are contained in six Schedules to the Bill. Each Schedule deals with a particular topic and related matters. The Schedules and their topics are:

- Schedule 1 – Australian Privacy Principles
- Schedule 2 – Credit reporting
- Schedule 3 – Privacy codes
- Schedule 4 – Other amendments of the Privacy Act
- Schedule 5 – Amendment of other Acts
- Schedule 6 – Application, transitional and savings provisions.[15]

Structure of this submission

11. The OAIC's comments on the Bill are structured as follows:

A. General issues in the APPs
B. Specific issues in the APPs
C. General Issues in the credit reporting provisions
D. Specific Issues in the credit reporting provisions
E. Specific issues on which the House of Representatives Standing Committee on Social Policy and Legal Affairs invited comment.

[14] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Explanatory Memorandum), p 1, available at http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813.
[15] Explanatory Memorandum, p 1-2.

A. General Issues in the APPs

Removing exceptions for agency-specific activities

12. In its APP submission, the OPC emphasised the importance of having a single set of high-level principles for the public and private sectors which promote national consistency[16] and minimise complexity.[17] Exceptions from the APPs for particular agencies increases the fragmentation of obligations between different sectors and entities and adds complexity to the principles. The inclusion of agency specific exceptions also creates complexity for the OAIC in its role as the regulator responsible for administering the Privacy Act, advising individuals of their privacy rights and educating entities on their new obligations.

13. The OAIC reiterates its view that where an exception is required for the specific personal information handling activities of agencies, this is more appropriately addressed in the agencies' enabling legislation[18] (thereby, bringing the information handling activity within the 'required or authorised by law' exception that exists in each of the relevant APPs).[19] The OAIC notes the Senate Committee's recommendation that the inclusion of agency specific provisions be reconsidered in light of this suggestion[20] and the Government Senate Committee APP Response which concluded that inclusion in an agency's enabling legislation is not appropriate.[21]

14. As an alternative to inclusion in an agency's enabling legislation, an agency could request that the Commissioner make a Public Interest Determination (PID) to suspend the operation of specific APPs in relation to activities that are in the public interest.[22]

15. The inclusion of specific authorisations in enabling legislation for acts or practices that would otherwise breach the APPs, or the making of a PID, would better ensure that individuals and members of the public are aware of the specific activities and purposes for which agencies may handle their personal information; ensure that any exemptions to the APPs are necessary and not broader than required; and increase agencies' accountability for their activities.

16. The OAIC suggests that since the Privacy Act does not currently contain agency specific exceptions, the activities and practices which the exceptions are intended to address can presumably already be undertaken in compliance with the Privacy Act. This view is supported by the Government Senate Committee APP Response, which indicated that the agency specific exceptions in the Bill are not new exceptions to

[16] APP Submission, para vi.
[17] APP Submission, para 11.
[18] APP Submission paras 24, 71-77.
[19] See APP 3.4(a), APP 3.6(a), APP 6.2(b), APP 8.2(c), APP 9.2(c), APP 12.2 and APP 12.3(g).
[20] APP Report, recommendation 2.
[21] Government Senate Committee APP Response, pp 3-4.
[22] See s 72 *Privacy Act 1988* (Privacy Act).

existing privacy laws, but rather are intended to clarify the interaction between agencies' existing functions and the APPs.[23] In this regard, the agency specific exceptions appear unnecessary. The application of the APPs could be effectively addressed in guidance issued by the OAIC.

17. If agency specific exceptions are retained in the Bill, the OAIC recommends that these exceptions should be subject to rules made by the Commissioner. This would ensure that the information handling needs of specific agencies are met, whilst also ensuring that any information handling permitted by the exception is confined to clearly defined circumstances and is carried out in a consistent and transparent manner.

18. The OAIC's comments on particular agency-specific exceptions are set out below.

Permitted General Situation (PGS) 6 – exception for consular and diplomatic functions and activities

19. The Bill creates exceptions to the obligations in relation to the collection, use and disclosure of personal information in the APPs where a 'permitted general situation' (PGS) exists. A 'permitted general situation' is defined in clause 16A in Schedule 1 of the Bill.

20. PGS 6 provides an exception to the requirements of APP 3.3 (in relation to the collection of sensitive information), APP 6.1 (in relation to the disclosure of personal information for a secondary purpose) and APP 8.1 (in relation to the cross boarder disclosure of personal information) where an agency reasonably believes the collection, use or disclosure of personal information is necessary for the agency's consular or diplomatic functions or activities. This exception has particular implications for the Department of Foreign Affairs and Trade's (DFAT) handling of personal information in the context of its consular and diplomatic functions. However, it is unclear whether the exception would also extend to other agencies that may engage in consular or diplomatic activities.

21. The effect of the exception in PGS 6 is to remove restrictions on the collection, use and disclosure of personal information where the agency reasonably believes the collection, use or disclosure is necessary for the agency's consular or diplomatic activities or functions. The intended scope of the exception in PGS 6, and the specific information handling practices of 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.

[23] Government Senate Committee APP Response, p 4.

22. The OAIC recommends removing the exception in PGS 6. 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, for the reasons at paragraph 15 above, 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 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.

23. Alternatively, if PGS 6 is retained in the Bill, the OAIC recommends that the exception should be subject to rules made by the Commissioner as with the 'missing persons' exception in PGS 3.[24]

Permitted General Situation (PGS) 7 – Defence Force exception

24. PGS 7 provides an exception to the same provisions as PGS 6 (see paragraph 20 above), but applies where the 'Defence Force'[25] reasonably believes that the collection, use or disclosure of personal information is necessary for a range of national security and humanitarian activities occurring outside of Australia. The OAIC believes that these circumstances may provide a compelling argument for not insisting on compliance with the requirements of the APPs as it may not be in the public interest.

25. However, the OAIC reiterates its view that, for the reasons at paragraph 15 above, these information handling activities are more appropriately addressed in the relevant agencies' enabling legislation, or alternatively under the Commissioner's power to make a PID. Accordingly, the OAIC recommends removing the exception in PGS 7. Alternatively, if PGS 7 is retained in the Bill, the OAIC recommends that the exception should be subject to rules made by the Commissioner as with the 'missing persons' exception in PGS 3.[26]

The inclusion of the Immigration Department in the definition of an 'enforcement body'

26. Item 17 of the Bill includes the 'Immigration Department'[27] within the definition of an 'enforcement body' and has the effect of bringing the Immigration Department within the enforcement related exceptions that appear throughout the APPs.[28] 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.

[24] See clause 16A(2) in Schedule 1 of *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (the Bill).
[25] 'Defence Force' is defined in s 6(1) Privacy Act to include 'the Australian Navy Cadets, the Australian Army Cadets and the Australian Air Force Cadets'.
[26] See clause 16A(2) in Schedule 1 of the Bill.
[27] The term 'Immigration Department' is defined at item 26 of Schedule 1 of the Bill.
[28] See APP 3.4(d), APP 6.2(e), APP 8.2(f), APP 9.2(e) and 12.3(i).

27. The OAIC notes that the Immigration Department is not currently an enforcement body under the Privacy Act, and was not included as an enforcement body in the Exposure Draft APPs. The OAIC understands that the Immigration Department has been included as an enforcement body to address its concerns about its ability to handle 'sensitive information'.

28. The Immigration Department would appear to be of a different character to the other agencies included within the definition of an 'enforcement body',[29] 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 PID. The OAIC recommends that the Immigration Department be removed from the definition of 'enforcement body'.

Replacing 'reasonably necessary' with 'necessary'

29. The objective standard of 'reasonably necessary' is adopted throughout the APPs.[30] In a number of instances this replaces the objective standard of 'necessary' that is used in the equivalent provisions in the IPPs and the NPPs.[31]

30. In its APP Submission, the OPC outlined a number of concerns regarding the use of the term 'reasonably necessary' in the Exposure Draft APPs. These concerns, which have not been addressed in the Bill, relate to:

- the introduction of 'reasonably necessary' in the new collection test (APP 3), which could unintentionally broaden the scope for collection and lessen the protection provided in the current IPP and NPP requirements
- multiple interpretations of 'reasonably necessary' in different APPs
- varied formulations of tests relating to necessity.[32]

31. The OAIC acknowledges that the Explanatory Memorandum clarifies that the term 'reasonably necessary' is to be interpreted objectively and in a practical sense, and is not intended to provide a lower level of protection compared with the NPPs, where an objective test is implied.[33] The OAIC notes that its existing guidance on the NPPs states that the Commissioner interprets 'necessary' in a practical sense,[34] and that the ALRC Report 108 found that the requirement that collection be 'necessary' implies an objective test.[35]

[29] For the existing definition of an 'enforcement body' see s 6(1) Privacy Act; the OAIC also notes that items 15 – 19 of Schedule 1 of the Bill add CrimTrac, the Immigration Department, the Office of the Director of Public Prosecutions (or a similar body established under a law of a State or Territory) and the Corruption and Crime Commission of Western Australia to the definition of an 'enforcement body' contained in s 6(1) Privacy Act.
[30] See, for example, APP 3.1, APP 3.2, APP 3.3 APP 6.2(e), APP 8.2(f) and APP 9.2.
[31] See for example, IPP 1.1, NPP 1.1, NPP 2.1(f), NPP 7.2 and NPP 10.1(e).
[32] APP Submission, para 25.
[33] Explanatory Memorandum, p 53.
[34] The former OPC 2001, *Guidelines to the National Privacy Principles* (NPP Guidelines), p 27, available at http://www.privacy.gov.au/materials/types/guidelines.
[35] ALRC Report 108, para 21.72.

32. Given that the term 'necessary' implies an objective test and that 'reasonably necessary' is intended to provide a comparable level of protection, the use of the phrase 'reasonably necessary' in place of the term 'necessary' adds unnecessary complexity to the APPs. Further, the APPs, as currently drafted in the Bill, use both the terms 'necessary' and 'reasonably necessary'. If the intention is for both terms to provide the same level of protection, the OAIC considers that retaining both creates uncertainty and is potentially confusing.

33. For simplicity and clarity, the OAIC recommends replacing the phrase 'reasonably necessary' with the term 'necessary' throughout the APPs. This change would also assist in addressing the other outstanding issues raised by the OPC in its APP Submission (see paragraph 30 above), and create greater certainty.

Removing the subjective standard 'believes' from exceptions

34. A number of exceptions to the restrictions on the collection, use and disclosure of personal information in the APPs require only that the entity 'reasonably believes' that the collection use and disclosure is necessary for the relevant activity. The OAIC notes, in particular:

- the exceptions in PGS 6 (consular and diplomatic exception) and PGS 7 (the Defence Force exception)
- the exception in relation to the collection of sensitive information by an 'enforcement body' in relation to its 'enforcement related activities'.[36]

35. The OAIC suggests that the inclusion of the subjective element 'believes' in these circumstances may result in the threshold being set too low. The reasons why a subjective element may be inappropriate in relation to these exceptions are set out below. These comments are subject to earlier recommendations relating to PGS 6 and PGS 7 (see paragraphs 19-25).

PGS 6 (consular and diplomatic exception) and PGS 7 (the Defence Force exception)

36. The OAIC is of the view that subjectivity created by the 'reasonable belief' qualification that has been introduced for the exceptions in PGS 6 and PGS 7 poses regulatory and compliance challenges and reduces the level of accountability to which those agencies are held.

37. The OAIC suggests that the agencies to which the exceptions in PGS 6 and PGS 7 apply should be able to determine whether the collection is 'necessary' for their *own* functions and activities (rather than 'reasonably believe' the collection is necessary), as do other agencies collecting personal information. In circumstances where these exceptions have the potential to apply in a broad range of circumstances (see paragraphs 21 and 24 above) the OAIC considers that a subjective standard is inappropriate. It could further reduce agencies' accountability for their activities and make it more difficult for individuals to dispute the collection, use and disclosure of their personal information.

[36] See APP 3.4(d).

Exception to collection for 'enforcement related activities' of 'enforcement bodies'

38. In relation to the exception to the collection of sensitive information for the 'enforcement related activities' of an 'enforcement body' the OAIC is concerned that the inclusion of a subjective standard may reduce existing privacy protections.

39. In circumstances where the definition of 'enforcement related activities' has been extended by item 20 of Schedule 1 of the Bill, and is framed to include a broad range of activities, such as surveillance, intelligence and monitoring activities, this exception has the potential to authorise the collection of a further broad category of sensitive information. In addition, given that sensitive information is recognised as requiring stricter protections than other types of personal information, the OAIC considers that the entity that holds the sensitive information should be required to make an objective assessment of whether it is necessary to collect the information without consent.[37]

40. For these reasons, the OAIC recommends amending the wording of PGS 6, PGS 7 and APP 3.4(d) by removing the words 'reasonably believes' and instead relying on the objective standard of 'necessary' (in line with the recommendation at paragraph 33 above). This would limit the breadth of the exceptions, better ensure appropriate privacy protection of individuals' personal information and be consistent with the objective standard used in other parts of the Bill.

Using consistent standards for agencies and organisations

41. The OAIC supports the simplification of the Privacy Act through the consolidation of the NPPs and the IPPs into a single set of high-level principles – the APPs. Additionally, the OAIC supports consistent information handling standards for agencies and organisations; this promotes national consistency and avoids adding unnecessary complexity to the APPs, making them simpler to understand and apply.

42. The OAIC considers that the different standards that apply to agencies and organisations in relation to the collection of personal information in APP 3 ('collection of solicited personal information') are unnecessary. APP 3 enables an organisation to collect personal information where it is 'reasonably necessary' for its functions or activities. However, an agency is able to collect personal information where it is 'reasonably necessary for, or directly related to' the agency's functions or activities. The OAIC believes that a requirement that the collection be 'necessary' (in accordance with the recommendation at paragraph 33 above) is sufficient for both agencies and organisations.

[37] ALRC Report 108, Recommendation 22-1; Government first stage response, p 42; see also Explanatory Memorandum, p 54.

43. In relation to the 'reasonably necessary' standard, the Explanatory Memorandum states that if an agency or organisation cannot, in practice, effectively pursue a legitimate function or activity, then the collection of that personal information would be regarded as necessary for that legitimate function or activity. It goes on to state that the 'directly related to' test is retained for agencies because there may be agencies that need to collect personal information in order to carry out legitimate and defined functions or activities, but may not be able to meet the reasonably necessary test.[38]

44. If specific instances arise where agencies are required to collect personal information that do not meet the 'reasonably necessary' test, and no exception applies, then the OAIC considers that other alternatives to authorise that collection, such as the inclusion of provisions in the relevant agency's enabling legislation or the Commissioner's power to make a PID[39] , are preferable.

45. Accordingly, the OAIC recommends removing the words 'directly related to' from APP 3.1, APP 3.3(a)(i) and APP 3.4(d)(i). This would reduce complexity and ensure that appropriate and consistent information handling practices apply to both agencies and organisations. This would also reflect the ALRC's recommendation and the Government's first stage response.[40]

Clarifying the meaning of 'Australian link'

46. Section 5B(3) of the Privacy Act (as amended by items 5, 6 and 7 of Schedule 4 of the Bill) outlines the circumstances in which an organisation or small business operator will have an 'Australian link'. Under s 5B(3)(c) an 'Australian link' will exist where the 'personal information was collected or held by the organisation or operator in Australia or an external Territory', and the other requirements of s 5B(3) are satisfied. The OAIC is concerned that the meaning of 'in Australia' in this provision is unclear, particularly in the online context.

47. The meaning of 'Australian link' has particular relevance and importance to the OAIC as the Privacy Act regulator. The Bill amends the Privacy Act so that it extends 'to an act done, or practice engaged in, outside Australia and the external territories by an agency, organisation or small business operator that has an Australian link'.[41] Effectively, the meaning of 'Australian link' will determine the entities subject to the Privacy Act against whom the Commissioner can exercise his or her enforcement powers. (The term 'Australian link' is also used in the credit reporting provisions in Schedule 2 of the Bill, and the OAIC comments on its use in those provisions at paragraphs 73 - 79 below).

48. The OAIC acknowledges that the Explanatory Memorandum clarifies that the reference to 'in Australia' in paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or

[38] Explanatory Memorandum, p 75.
[39] See s 71 Privacy Act.
[40] ALRC Report 108, recommendation 21-5; Government first stage response, p 42.
[41] See item 2 of Schedule 4 of the Bill.

an external territory by an overseas entity, and that this would include collection from an individual physically located in Australia over the internet by a company which has no physical presence in Australia.[42] However, this intended meaning is not clear on the face of the Bill.

49. Given its importance in determining whether obligations under the Privacy Act apply, and to provide certainty for entities and the OAIC as the Privacy Act regulator, the OAIC recommends the meaning of 'in Australia' in s 5B(3)(c) be made explicit; for example, by amending 'in Australia' to 'from Australia'.

B. Specific Issues in the Australian Privacy Principles

APP 3.4(e) - exception to collection of sensitive information for non-profit organisations

50. APP 3.4(e) provides an exception to the collection of sensitive information for non-profit organisations (NPOs). One of the criteria that must be satisfied for the exception to apply is that the personal information 'relates to' the activities of the NPO.[43]

51. The OAIC considers that the 'relates to' test sets a lower threshold than the 'reasonably necessary' requirement used elsewhere in APP 3 it therefore could permit the collection of sensitive information in a broader range of circumstances. The reasons why NPOs would require this lower threshold is not evident to the OAIC. In particular, it is not clear what activities undertaken by NPOs would be prevented by requiring that the collection of sensitive information be 'necessary for' the activities of the NPO. As noted at paragraphs 43 - 44 above, a requirement that the collection of the relevant information be 'necessary for' the activities of the relevant entity would allow for the collection of information that is necessary to pursue the entity's legitimate functions and activities, and is interpreted in an objective and practical manner.

52. The OAIC acknowledges that for the exception in APP 3.4(e) to apply to the collection of sensitive information by an NPO, the information must also relate solely to the members of the NPO, or to individuals who have regular contact with the NPO. While this narrows the exception in terms of the individuals about whom sensitive information may be collected, it does not confine the circumstances in which the information can be collected about those individuals by the NPO.

53. The OAIC considers that the range of those circumstances, as permitted by the 'related to' test in APP 3.1(e)(i), appear unnecessarily broad. This is particularly so given that:

- the exception relates to the collection of 'sensitive information' – a category of information that is recognised as requiring more stringent levels of protection

[42] Explanatory Memorandum, p 219.
[43] See APP 3.3(e)(i).

- the definition of NPO has been amended to include a broader class of organisations. [44]

54. The OAIC therefore recommends amending APP 3.4(e)(i) to require that the information be 'necessary for' the NPO's activities (consistent with the recommendation at paragraph 33 above). This would ensure that the exception is appropriately limited, that appropriate protection is accorded to individual's sensitive information, and would be consistent with the standard in other exceptions, including those in APP 3.[45]

APP 3.5 – the requirement that a collection is not 'unreasonably intrusive'

55. While APP 3 requires that an APP entity collect personal information by lawful and fair means,[46] it does not contain a requirement that the collection be in a way that is not unreasonably intrusive. The inclusion of a requirement to collect information in a way that is not unreasonably intrusive is present in both the NPPs and IPPs,[47] and is important in ensuring that information collection practices take account of the cultural sensitivities of different communities and groups within Australia.

56. For example, there exist some categories of personal information that are particularly sensitive for Indigenous Australians because of their cultural context, for example, the name of a deceased person. In many Indigenous Australian communities, it is inappropriate to ask close relatives to discuss, write down, or see written down the name of a person who has passed away. Instead, it may be appropriate to seek the consent of the individual to collect the personal information from another source.[48] Accordingly, it is important that the APPs ensure that information handling practices take account of these cultural sensitivities by, for example, requiring that personal information is not collected in an 'unreasonably intrusive manner'.

57. Although the Explanatory Memorandum clarifies that collection by 'fair means' in APP 3.5 would also extend to an obligation not to use means of collection that are unreasonably intrusive,[49] this is not clear on the face of the Bill. For clarity and certainty, the OAIC therefore recommends that APP 3.5 be amended to include a specific reference to the obligation not to collect information in a way that is unreasonably intrusive.

[44] See item 31 of Schedule 1 of the Bill; Explanatory Memorandum, p 60.
[45] See for example, the 'Permitted General Situation' (PGS) exceptions under APP 3.4(b).
[46] See APP 3.5.
[47] See IPP 3(d) and NPP 1.2.
[48] The former OPC 1998, *Australian Government agencies in the Northern Territory - Indigenous Protocol*: *Minding Your Own Business*, p 2, available at http://www.privacy.gov.au/materials/types/guidelines.
[49] Explanatory Memorandum, p 77.

APP 6.3 – the disclosure of 'biometric information and biometric templates' by an agency to an 'enforcement body'

58. APP 6.3 creates an exception to the general rule that an APP entity must not disclose personal information for a secondary purpose without the consent of the individual to whom the information relates.[50] APP 6.3 permits an agency that is not an 'enforcement body' to share 'biometric information or biometric templates' with an 'enforcement body' provided that the disclosure is conducted in accordance with guidelines made by the Commissioner.

59. The OAIC notes that the exceptions in APP 6.2 already permit information sharing in a wide range of circumstances, including where an agency reasonably believes that the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.[51] Further, the definition of 'enforcement related activities' has been extended by item 20 of Schedule 1 of the Bill to include a broad range of activities, such as surveillance, intelligence and monitoring activities (see paragraph 38 above).

60. Given the range and breadth of the exceptions in APP 6.2, particularly the exception in APP 6.2(e), the OAIC does not consider that a further exception is necessary. If there are particular instances where agencies need to share biometric information or biometric templates with enforcement bodies that are not otherwise permitted by the APPs, then (for the reasons at paragraph 15 above) they should be dealt with in agencies' enabling legislation or under the Commissioner's power to make a PID.[52]

61. The OAIC acknowledges that the guidelines made by the Commissioner with which the disclosure must comply may provide additional requirements that restrict the sharing of biometric information and biometric templates. However, the OAIC is unaware of appropriate additional parameters that could be imposed by the guidelines, beyond limiting disclosure to the types of circumstances that are already permitted under APPs 6.1 and 6.2.

62. The OAIC therefore recommends removing the exception in APP 6.3.

63. However, if the exception is retained in the Bill, the OAIC recommends replacing the reference to 'guidelines' in APP 6.3(d) with 'rules',[53] in accordance with:

    - the ALRC's recommendation 47-2 (accepted by the Government in its first stage response)[54] that where a breach of the guidelines would constitute an interference with privacy they should be called 'rules'[55]

[50] See APP 6.1.
[51] See APP 6.2(e).
[52] See s 71 Privacy Act.
[53] The OAIC notes that if this amendment is made, the reference to 'guidelines' in clause 28(1)(b) of the Bill should also be replaced with 'rules'.
[54] Government first stage response, p 85.
[55] ALRC Report 108, para 47.36.

- the Explanatory Memorandum, which states that:

  The word 'rule' will be used where appropriate throughout the Privacy Act to more accurately reflect the binding nature of certain guidelines and to distinguish binding instruments issued or approved by the Commissioner from voluntary guidance.[56]

The guidelines referred to in APP 6.3 are binding, and a disclosure that breached the guidelines would be an interference with privacy under s 13 of the Privacy Act (as amended by item 42 of Schedule 4 of the Bill). The OAIC understands that the reference to 'guidelines' instead of 'rules' in this provision was an unintentional oversight.

APP 8.2(e) – exception for disclosures under international agreements relating to information sharing

64. APP 8.1 requires an entity that discloses personal information to an overseas recipient to take reasonable steps to ensure that the overseas recipient does not handle the information in a way that would breach the APPs. In addition, where APP 8.1 applies, the entity remains accountable for the way in which the overseas recipient handles the information.[57]

65. APP 8.2(e) provides an exception to these requirements if the disclosure is by an agency and is 'required or authorised by or under an international agreement relating to information sharing to which Australia is a party'. The Explanatory Memorandum clarifies that this exception is intended to include all forms of information sharing agreements made between Australian and international counterparts, for example, treaties and exchange of letters.[58]

66. The OAIC understands that an international agreement does not have any direct legal effect in Australia until it is incorporated into domestic law by statute,[59] and that a treaty that has not been implemented through domestic legislation can affect neither rights nor obligations in Australian law.[60]

67. The OAIC suggests that, wherever practicable, specific domestic legislative authority should be the basis for the exception in relation to the overseas disclosure of personal information under an international agreement.[61] Alternatively, such disclosures may be the subject of a PID made by the Commissioner.[62]

[56] Explanatory Memorandum, pp 220, 221, 227, 261 and 266.
[57] See clause 16C in Schedule 1 of the Bill.
[58] Explanatory Memorandum, p 85.
[59] *Minister for Immigration and Ethnic Affairs v Ah Hin Teoh* (1995) 183 CLR 273 at 286-8 per Mason CJ and Deane J, at 298 per Toohey J, at 315 per McHugh J.
[60] LexisNexis, *Halsbury's Laws of Australia,* vol 14 (at 6 June 2012) 215 '1 International Law and Relations' [215-55].
[61] In those circumstances the 'required or authorised by or under law' exception in APP 8.2(c) would apply.
[62] See s 71 Privacy Act.

68. This would ensure that the circumstances where an agency will not be required to comply with APP 8.1, or the accountability requirements in clause 16C of the Bill, are subject to sufficient scrutiny.

69. The OAIC therefore recommends removing the exception in APP 8.2(e).

C. General Issues in the credit reporting provisions

The inclusion of Part IIIA in a Schedule to the Act

70. In its Credit Reporting Submission, the OAIC recommended including the credit reporting provisions in a Schedule to the Act.[63] The Senate Committee, in its Credit Reporting Provisions Report, stated that:

> *'there is merit in considering whether the complexity of the consumer credit provisions can be reduced, and the provisions can be more readily accessible and understood, if the provisions were contained in a schedule to the Privacy Act'.*[64]

71. Under the Bill, the new credit reporting provisions will be retained in the main body of the Privacy Act. In contrast, the APPs will be contained in a Schedule to 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.[65] 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.

72. Noting the Senate Committee's comments, and for consistency with the approach taken in relation to the APPs, the OAIC recommends including the credit reporting provisions in Part IIIA of the Privacy Act (as amended by Schedule 2 of the Bill) in a Schedule to the Act.

Excluding foreign credit and foreign credit providers from the credit reporting system

73. The OAIC notes the Government's intention that the credit reporting system should not contain any foreign credit information or information from foreign credit providers, even if they have provided credit to an individual in Australia, and that the credit reporting system should not be able to be accessed by foreign credit providers.[66]

---

[63] The former OPC 2011, *Submission to the Senate Finance and Public Administration Committee on the Exposure Draft credit reporting provisions* (Credit Reporting Submission), para 20.
[64] Senate Finance and Public Administration Committee 2011, *Report Part 2 – Credit Reporting* (Credit Report) para 3.20, available at http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=fapa_ctte/priv_exp_drafts/index.htm.
[65] Explanatory Memorandum, at p 2.
[66] Explanatory Memorandum, at pp 91-92.

74. The Explanatory Memorandum states that the Government considered giving effect to these policies by setting out the limitations in a number of general provisions.[67] The Explanatory Memorandum goes on to say that it was considered that a simpler, clearer and more effective approach was to impose limitations on each provision dealing with the collection, use and disclosure of information by credit reporting bodies (CRB) and credit providers. Accordingly, the Bill seeks to give effect to this intention by requiring, in each relevant provision dealing with the collection, use and disclosure of information by CRBs and credit providers, that the relevant entity have an 'Australian link', or that the relevant information relates to credit that has been 'provided, or applied for, in Australia'.

75. The OAIC considers that this approach may create uncertainty and complexity, and have a number of unintended consequences with the result that the intention to exclude foreign credit and foreign credit providers may not be achieved. This is because the application of the term 'Australian link' could make the credit provisions apply to foreign entities in certain circumstances.

76. If the intention is to exclude foreign credit and foreign credit providers, the OAIC suggests that it is not appropriate for entities that meet the definition of 'Australian link' in s 5B(3) (as amended by items 5-7 of Schedule 4 of the Bill) to participate in the credit reporting system.

77. While the OAIC notes that the Explanatory Memorandum suggests that the term 'Australian link' will have a slightly different operation when it is applied to the credit reporting provisions, as opposed to other parts of the Privacy Act, it is unclear how this is meant to apply in the context of the credit provisions.[68]

78. In addition, the operation of clause 20C(4) of the Bill may also be inconsistent with the Government's intention. It provides an exception to the prohibition on a CRB collecting credit information about an individual. One of the criteria that must be satisfied for the exception to apply is that the information must relate to 'credit that is or has been provided or applied for*, in Australia'* (emphasis added). The OAIC notes that the term 'in Australia' is also used in the definition of 'Australian link' in s 5B(3) of the Privacy Act. Consistent with the interpretation of the term 'in Australia' referred to in the Explanatory Memorandum when it is used in the definition of 'Australian link' (see paragraph 48 above), the OAIC is concerned that an individual who makes an online application for credit to a foreign entity while physically located in Australia, could be considered to have applied for that credit in Australia. The OAIC therefore suggests that clause 20C(4) may allow information about credit provided by an overseas entity to be included in the credit reporting system.

79. Given these matters, the OAIC recommends that, in order to give effect to the Government's intention to exclude foreign credit and foreign credit providers, they

[67] Explanatory Memorandum, p 91.
[68] Explanatory Memorandum, p 92.

be explicitly excluded by specific provisions in the Bill. The OAIC considers that such an approach would create greater clarity and certainty, and more effectively achieve the Government's intention.

D. Specific Issues in the credit reporting provisions

The process for individuals to correct their credit related information

80. Schedule 2 of the Bill gives an individual the right to request a CRB or credit provider to have their credit information corrected.[69] An individual may make this request to any CRB or credit provider that holds their credit-related personal information, even if the CRB or credit provider does not hold the particular item of information the individual is seeking to have corrected.[70]

81. A CRB or credit provider that receives a correction request from an individual must take reasonable steps to correct the information where it is satisfied that the personal information is inaccurate, out-of-date, incomplete, irrelevant or misleading.[71] Additionally, a CRB or credit provider that receives a correction request must notify various entities if it corrects the relevant information, and also if it does not correct the relevant information.[72]

82. The OAIC is concerned to ensure that where the CRB or credit provider that receives the correction request does not hold the specific item of credit information that the individual is seeking to have corrected, the correction and notification obligations are clear, appropriate and comprehensive. In those circumstances, it 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
- 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.

83. There is uncertainty as to whether the provisions in the Bill achieve this. The OAIC does not consider that the Explanatory Memorandum is sufficient to resolve the uncertainty. Specifically:

- whether the obligation on the CRB or credit provider that receives the correction request to take reasonable steps to 'correct the information', includes an obligation to take reasonable steps to have the information

[69] See clauses 20T and 21V of Schedule 2.
[70] See clauses 20T(1) and 21V(1) of Schedule 2; see also Explanatory Memorandum, pp 148-149.
[71] See clauses 20T(2) and 21V(2) of Schedule 2.
[72] See clauses 20U and 21W of Schedule 2.

corrected where the CRB or credit provider does not hold the relevant information.[73]

- whether the obligation to take reasonable steps to notify certain entities when personal information is corrected applies to a CRB or credit provider that received a correction request and the information is corrected by another entity (because the CRB or credit provider does not hold the inaccurate, out of date, incomplete, irrelevant or misleading information). If not, the OAIC understands that the Bill does not place an obligation on any entity to notify the individual that the information has been corrected, since those notification obligations only apply to the entity that received the correction request.[74]
- how the obligation to take reasonable steps to notify certain entities when the CRB or credit provider 'does not correct' personal information applies to a CRB or credit provider that does not itself hold the personal information. For example, does the obligation apply where another entity that holds the information corrects the information, but the CRB or credit provider does not itself correct any information because it does not hold the information? Does it apply where some, but not all the entities that hold the information, correct the information?

84. The OAIC is of the view that the Bill is unclear on each of these issues and recommends that the Bill be amended to ensure that the correction provisions are clear, and operate effectively.

E. Specific issues on which the House of Representatives Standing Committee on Social Policy and Legal Affairs invited comment

85. The OAIC notes that the House of Representatives Standing Committee on Social Policy and Legal Affairs has invited particular comment on whether:
    - defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections
    - provisions [of the Bill] relating to use of depersonalised data are appropriate.[75]

[73] Such steps might include, at a minimum, notifying the entity that holds the information, and requesting that they correct the information. On receiving that notification, the relevant entity may be required to correct the information under either the correction obligations in Pt IIIA (if it is a CRB or credit provider), or the APPs (if it is an APP entity); see APP 13 and clause 20S in Schedule 2 of the Bill (for CRBs) and clause 21U in Schedule 2 of the Bill (for credit providers). The OAIC acknowledges that the extent to which the CRB or credit provider must take steps to determine which entities hold the relevant information and to have them correct the information may depend on the circumstances.

[74] The OAIC notes that the notification obligations that apply to entities that correct information under clauses 20U and 21U do not require the individual to whom the information relates to be notified of the correction.

[75] Email from Social Policy and Legal Affairs Committee to OAIC Enquiries, 10 July 2012.

Inadvertent disclosures

86. The Bill only permits entities to disclose personal information in certain circumstances.[76] The Bill also requires entities to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure.[77]

87. A disclosure in contravention of these requirements will be an interference with the privacy of an individual under s 13 of the Privacy Act (as amended by item 42 of Schedule 4 of the Bill). An entity that interferes with the privacy of an individual may, for example and depending on the circumstances, be liable to do an act or practice to redress any loss or damage suffered by the individual,[78] pay compensation to the individual[79] or pay a civil penalty.[80] The OAIC notes that in each instance, the appropriate remedy or penalty awarded by the Commissioner or the court is discretionary.

88. The OAIC does not support the availability of defences to contraventions of the Privacy Act (as amended by the Bill) for inadvertent disclosures. Rather, the OAIC considers that the circumstances of the disclosure, including whether the entity has taken reasonable steps to incorporate appropriate security protections into its systems, should be taken into account in determining the form and/or amount of any remedy or penalty.

Consistent and appropriate regulation of information used for credit research purposes

89. The Bill allows CRBs to use or disclose de-identified information for research purposes in certain circumstances, in compliance with rules made by the Commissioner.[81] CRBs are otherwise prohibited from using or disclosing de-identified information.

90. In its Credit Reporting Submission, the OAIC noted that this approach would be the first time that the Privacy Act would regulate the use or disclosure of de-identified information. Ordinarily, such information falls outside the Privacy Act's coverage as it is does not meet the definition of 'personal information'.[82]

91. In general, using de-identified information for research is potentially less privacy-invasive than using identified information, provided that:

    - where practicable, individuals are informed that information may be de-identified and used for research purposes (and that this aligns with individuals' reasonable expectations of use by the relevant sector), and

[76] See, for example, APP 6 ('use or disclosure of personal information').
[77] See, for example APP 11 ('security of personal information').
[78] See clause 52(1A)(1A)(c) in Schedule 4 of the Bill.
[79] See clause 52(1A)(1A)(d) in Schedule 4 of the Bill.
[80] See clause 80W in Schedule 4 of the Bill.
[81] See Clause 20M in Schedule 2 of the Bill.
[82] Credit Reporting Submission, para 73.

- the information is appropriately de-identified, used and otherwise handled in a way that minimises any potential for re-identification of individuals.[83]

92. The OAIC considers that if the handling of de-identified information for research purposes is to be regulated under the Bill, it is important that such regulation is consistent and appropriate. That is:

- in a way that is consistent with or complementary to research regulation in other areas of the Privacy Act (noting that new provisions relating to health and research are yet to be released)[84]
- with appropriate consideration of the types of information involved in the credit reporting system, its current usage by CRBs, and community sensitivities and expectations. The OAIC considers that requiring the CRB to comply with rules made by the Commissioner adequately addresses this consideration.

[83] The former OPC issued guidance on avoiding re-identification of individuals from de-identified information in another context; see former OPC 2001, *Private Sector Information Sheet 9 – 2001: Handling Health Information for Research and Management*, pp 3-4, available at http://www.privacy.gov.au/materials/types/infosheets/view/6568.

[84] The general content of those provisions are outlined in the Government first stage response, p 139.