Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Senate Standing Committee on Legal and Constitutional Affairs

on the

Privacy Amendment (Enhancing Privacy Protection) Bill 2012

9 July 2012

The Acting Privacy Commissioner wishes to acknowledge the work of Jason Forte, Senior Policy and Compliance Officer, in the preparation of this submission.

Office of the Victorian Privacy Commissioner (Privacy Victoria)
GPO Box 5057
10-16 Queen Street
Melbourne Victoria 3000
Australia
Phone: 1300-666-444
Fax: +61-3-8619-8700
Email: enquiries@privacy.vic.gov.au
Website: www.privacy.vic.gov.au

Introduction

1 The *Privacy Amendments (Enhancing Privacy Protection) Bill 2012* (**the Bill**) and the Australian Privacy Principles (**APPs**) have the potential to significantly impact on States and Territories (including Victoria), because of the proposed move toward uniform or "harmonised" legislation.[1] This is true both of the privacy rights of individual Victorians and the substance and structure of Victorian law, legislation and regulation. It is in this context that the following comments are made.

2 I made a submission in my then role of Deputy Privacy Commissioner to the Senate Standing Committee on Finance and Public Administration (**the Committee**) regarding the Exposure Draft of the APPs in July 2010, in which I expressed my concerns about the Draft, particularly regarding the complexity of the APPs. The concerns that I expressed in my 2010 submission have deepened, as it appears that the Committee's report on the Exposure Draft has had little effect on the re-drafting of the APPs. Indeed, while the Government has appeared to have accepted some of the comments made in submissions to that Committee in the Government's response to the Exposure Draft, it is unfortunate that most of those comments were not taken into account when drafting the Bill. The APPs have not been substantially altered and my concerns remain. Accordingly, many of the comments I made to that Committee are replicated in their entirety in this submission.

3 While much of the Bill is generally welcomed (such as the increased powers given to the Office of the Australian Information Commissioner) some of the changes, in conjunction with the complexity of the APPs, may prohibit the workability of the Bill and detract from the Bill's ultimate aim, which is to enhance the privacy protection of Australians.

Overview

Consistency, simplicity and clarity

4 Recommendation 18-1 of the Australian Law Reform Commission (**ALRC**)'s Report 108, *For Your Information: Australian Privacy Law and Practice* (2008), states:

> The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:
>
> (a) the obligations in the privacy principles generally should be expressed as high-level principles;
>
> (b) the privacy principles should be technology neutral;
>
> (c) the privacy principles should be simple, clear and easy to understand and apply; and

[1] See Australian Law Reform Commission (ALRC), *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), Recommendation 3.4, available at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/_3.html; Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, October 2009*, 'Towards National Consistency', 13.

(d) the privacy principles should impose reasonable obligations on agencies and organisations.[2]

5 In addition, Recommendation 1 of the Committee's Report in June 2011 recommended that:

> [t]he Department of the Prime Minister and Cabinet re-assess the draft Australian Privacy Principles with a view to improving clarity through the use of simpler and more concise terms and to avoid the repetition of requirements that are substantially similar.

6 It is unfortunate that, in my view, the APPs fail to fulfil these recommendations. While in parts the APPs are expressed as high-level principles, in others the level of detail and complexity works against this aim. This detail and complexity means the APPs are not, as a whole, simple, clear and easy to understand and apply.

7 For example, in my 2010 submission I noted that APP 8 contained nine separate and alternative exception clauses within the Principle. The Government seemingly accepted the Committee's comments about the re-drafting of some of the APPs in relation to these exceptions. However, the exceptions have now been described as "permitted general situations" and moved to the table section 16A, the effect of which is exactly the same as the previous drafting. I consider this needlessly complex compared with the Unified Privacy Principles drafted by the ALRC.

8 The Government did not accept the Committee's recommendation (Recommendation 2) that agency-specific provisions in the APPs should be dealt with in portfolio legislation. Failing to do so, however, means that certain APPs will have little, if any, utility if and when the APPs are incorporated into State or Territory legislation. A better approach would be to draft high-level, simple, lucid principles, which could equally apply to Commonwealth, State or Territory public sector agencies, local councils or private sector organisations. I reiterate my point from my previous submission that where one or more of these entities needed modification to or exemption from the specific APP, this could be done in a separate section of the *Privacy Act*,[3] rather than include those exceptions in the APP.

Structure

9 The intention that the order in which the APPs appear reflect what occurs as entities collect, hold, use and disclose personal information is welcome. However, as outlined above, the density of language and complexity of ideas embodied in the APPs as currently drafted undercuts, to some extent, the logic of this structural progression.

[2] ALRC, above n 1, Recommendation 18-1.
[3] As, for example, in section 13 of the *Information Privacy Act 2000* (Vic) in relation to law enforcement agencies.

The Australian Privacy Principles

APP 1 – open and transparent management of personal information

10 APP 1 has as its object that entities manage personal information in an open and transparent way. It requires that entities take reasonable steps to implement practices, procedures and systems that will ensure that the APP entity (public sector agency or private sector organisation) complies with the APPs and enables the entity to deal with enquiries and complaints. It will require that an entity's privacy policy specify whether the entity is likely to disclose personal information to overseas recipients and the countries in which the recipients are located, and if it is practicable to specify them.

11 This is considerably more prescriptive and detailed than the existing National Privacy Principle (**NPP**) 5 in the *Privacy Act 1988* (Cth) and Information Privacy Principle (**VIPP**) 5 in the *Information Privacy Act 2000* (Vic), which currently merely require large private sector organisations and Victorian public sector organisations respectively to have clearly expressed policies on managing personal information.

12 This is a welcome change, in that it will better allow individuals to identify precisely how entities intend to handle personal information.

13 However, in line with my comments on APP 8 (see below), my preference would be that entities always be required to determine and indicate which countries overseas recipients are located in, rather than only where this is "practicable". With the proliferation of cloud computing, this is an important consideration for individuals who wish to enter into transactions with entities in line with the objects of the Bill in section 2A. While I recognise that given current technologies like cloud computing, specifying the exact location may be difficult, organisations that seek to store or transfer data offshore should be held at a high standard in order to protect individuals' personal information. A requirement that entities tell individuals where their information is being held if offshore goes no further than requiring entities to disclose information which they should already know.

APP 2 – anonymity and pseudonymity

14 This APP provides that individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity, unless this is impracticable or the entity is required or authorised under a law to deal with individuals who have identified themselves.

15 VIPP 8 currently gives Victorians the option of transacting anonymously with Victorian public sector organisations wherever it is lawful and practicable to do so.[4]

[4] Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, Edition 3, November 2011, p 159-163, available at http://www.privacy.vic.gov.au/privacy/web2.nsf/files/guidelines-to-the-information-privacy-principles.

16 Where an organisation allows individuals to transact anonymously, the benefits are mutual. The individual transacts without giving up any control over his or her personal information. The entity will not incur any of the obligations that follow from collection of personal information under the other APPs. Where entities purport to collect and use anonymous data, they should ensure that the information is not reasonably identifiable or reasonably capable of being re-identified through, for example, linkage to other data sets. Providing an anonymity option is also consistent with the principle that an organisation or agency should not collect personal information unless this is necessary for one or more of its functions or activities.

17 In situations where it is necessary to determine that the individual involved in a particular transaction is the same one as has been involved in previous transactions without actually identifying the individual, pseudonymity is a desirable option.

APP 3 – Collection of solicited personal information

18 APP 3 applies to the collection of solicited information. It provides that personal information must not be collected unless it is reasonably necessary for, or directly related to, an entity's functions or activities. It also provides that an entity must collect information directly from an individual unless it is unreasonable or impracticable to do so. Sensitive information must not be collected except with consent (although there are exceptions to this rule).

19 The Government rejected the Committee's recommendation (Recommendation 8) to reconsider the use of the word "reasonably" in the "reasonably necessary" test. I again restate my concerns regarding the use of the terms "reasonably necessary" and "or directly related to" in APP 3. This is a weakening of current privacy protections and against the stated intention of the Bill, which is to improve privacy protections for individuals. The APPs should represent the highest standard of privacy protection currently enjoyed in Australia, not the lowest common denominator. Agencies or organisations should only collect personal information that is *necessary* for their functions or activities (as provided by the current VIPP 1.1 in the *Information Privacy Act*), not information that an agency or organisation reasonably believes may be necessary for their functions or activities, or which is directly related to them.

20 I note that in interpreting the meaning of 'necessity', the Victorian Civil and Administrative Tribunal has stated that "necessary" does not mean essential but rather "subjected to the top scale of reasonableness".[5] Consequently, an assessment of necessity involves considerations of reasonableness, but *objective* reasonableness as determined by a regulator or adjudicative body, and not subjectively by the collecting organisation. Similarly, the High Court has ruled that necessity refers to what is necessary in balancing competing rights and interests in a democratic society and that necessity does not mean unavoidable, essential or indispensable but rather a consideration of what is

---

[5] *Ng v Department of Education* [2005] VCAT 1054, para 77.

proportionate[6] or what may involve "close scrutiny, congruent with a search for 'compelling justification'".[7]

21 While the Government's response and the Explanatory Memorandum to the Bill explains that the test will be assessed from the perspective of a reasonable person (not merely from the perspective of the collecting entity), I do not agree that adding the word "reasonably" would result in an objective test. While it is difficult to determine precisely how collection of information will be affected, there remains a concern that, as currently drafted, APP 3 may result in the collection of unnecessary information. Similarly, I consider that the "directly related to" test will result in a lower threshold of collection, which is extremely concerning. The concept that only necessary information should be collected is the most essential and fundamental of all privacy principles.

22 In relation to sensitive information, APP 3.3(a) is of concern as, while this exception is similar to the existing exception in VIPP 10.1(b) of the *Information Privacy Act*, it is not as stringent. The APPs should represent the highest level of current privacy protection in Australia. I would support a narrower drafting of APP 3.3(a) in order to appropriately protect this class of personal information. VIPP 10.1(b) recognises organisations can collect sensitive information where collection is required under law. Unlike VIPP 2.1(f) which allows personal information to be used or disclosed where "required or authorised by or under law", VIPP 10.1(b) limits the authority for collection of sensitive information to when it is "required under law" – not when such collection is simply "authorised". The requirement to collect sensitive information must be mandatory, and not simply permissive or discretionary.[8] The drafting of APP 3.3(a) defeats the purpose of making sensitive information a special class of information, and will affect later uses and disclosures of this type of information.

23 As indicated earlier, listing exceptions that relate solely to Commonwealth agencies is problematic when expressly included in the APP itself, as this reduces the simplicity, lucidity and "high-level" nature of the APPs. As well as making them more difficult to understand, this reduces the ability of States and Territories to readily adopt them with minimal amendment.

24 APP 3.6 is strongly supported. Direct collection of personal information from the individual about whom the information relates is always preferable. Direct collection enables individuals to have some measure of control over what is collected, by whom and for what purposes. It provides individuals with an opportunity to refuse to participate in the collection or to provide their information on conditions or with reassurances about how it is to be used.

25 Direct collection also makes it more likely that the information organisations collect will be relevant, accurate and complete (and therefore more likely to assist organisations in

[6] *Mulholland v Australian Electoral Commission* [2004] HCA 41, 33-39 and 249-251.
[7] *Mulholland v Australian Electoral Commission* [2004] HCA 41, 39-40.
[8] Office of the Victorian Privacy Commissioner, *Guidelines*, above n 4, p 181-182.

complying with the requirements of APP 10), as firsthand information is less likely to suffer from the data quality problems usually associated with second-hand information.[9]

26 The 'reasonable and practicable' requirement is an important inclusion as it provides for the circumstances where it is not practically possible to collect information directly from the individual. This may occur, for example, where an individual discloses information about their family circumstances when applying for financial assistance or welfare benefits.[10]

27 I note that existing Guidelines produced by the Australian Privacy Commissioner on the National Privacy Principles provide some guidance on determining practicability and include consideration of:

- whether it is possible to collect the information directly;
- whether a reasonable individual might expect information about them to be collected directly or indirectly;
- how sensitive the information is;
- the cost to an organisation of collecting directly rather than indirectly;
- the privacy consequences for the individual if the information is collected indirectly rather than directly; and
- what is accepted practice (by consumers and the industry).[11]

28 To this I would add that 'practicable' connotes an element of reasonableness and prudence. In this context, 'practicable' should mean capable of being done or feasible.[12]

29 Further guidance, which clarifies the types of circumstances in which it would not be reasonable and practicable to collect information directly from individuals, should be jointly prepared by all Privacy (or Information) Commissioners across jurisdictions. Such guidance material should include reference to relevant case law.[13]

APP 4 – receiving unsolicited information

30 APP 4 applies to unsolicited information. It provides that when an entity receives unsolicited personal information, it must, within a reasonable period, determine whether it could have collected that information under APP 3. If so, it must treat that information in accordance with APPs 5 to 13. If not, it must destroy or effectively de-identify that information.

[9] Ibid, p 43.
[10] Ibid, p 43.
[11] Office of the Australian Privacy Commissioner, *Guidelines to the National Privacy Principles,* (2001) p 31-2.
[12] Office of the Victorian Privacy Commissioner, above n 4, p 25.
[13] See, for example, *Seven Network (Operation) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637.

31 It has been suggested that APP 4 may increase the burden on certain organisations which receive a significant amount of unsolicited information as it requires an assessment of the information. The VIPPs do not currently explicitly deal with this situation, as VIPP 1 makes no distinction between solicited and unsolicited information. In general, however, APP 4 reflects the interpretation and approach adopted by the Victorian Privacy Commissioner and is welcomed.[14] Entities should be required to assess and deal with unsolicited information in a way consistent with other APPs.

APP 5 – notification of the collection of personal information

32 This APP requires that entities provide privacy notification statements when, before, or as soon as practicable after, collecting personal information. In addition to providing notice about matters such as the purpose of collection and to whom the information may be disclosed (and other matters that currently must be notified under NPP 1 and VIPP 1), an entity will be required to notify additional matters. These include the circumstances of collection if the entity has not collected that information directly from the individual, whether the entity is likely to disclose personal information to overseas recipients and the countries in which the recipients are located, if it is practicable to specify them.

33 I strongly support APP 5. Giving notice is essential for promoting transparency about an organisation's collection and handling of personal information, and for ensuring that individuals are aware of their rights and obligations in respect to giving up (and later accessing) their information.[15] A privacy policy and other information provided to individuals through an 'openness' privacy principle should be distinguished from providing 'notice' to individuals when collecting their personal information. While a privacy policy will often be useful in proving general information about how an organisation handles personal information, it may not be comprehensive enough to inform individuals about all the matters covered by a separate notification privacy principle.

34 Notice statements under a notification privacy principle are generally more tailored to the particular collection practice, as opposed to the more general statements about all types of information handling practices that organisations engage in, as required under an 'openness' or 'transparency' privacy principle, like APP 1.[16]

APP 6 – use or disclosure of personal information

35 APP 6 provides for the general rule that personal information can be used or disclosed for the purpose for which it was collected, or a related (or in the case of sensitive information, directly related) purpose that the affected individual would reasonably expect. A number of exceptions to this general rule apply, for example, if the individual has consented to use or disclosure for another purpose, or where the use or disclosure is

[14] See Office of the Victorian Privacy Commissioner, above n 4, p 30-31.
[15] Ibid, p 38.
[16] Ibid, p 39. See also, Office of the Victorian Privacy Commissioner, Information Sheet 02.11, *Collection Notices* (March 2011) and Information Sheet 01.11, *Drafting and Reviewing a Privacy Policy* (March 2011), available at http://www.privacy.vic.gov.au.

reasonably necessary for the establishment, exercise or defence of a legal or equitable claim, or a confidential alternative dispute resolution. In this, it largely mirrors the existing provisions of NPP 2 and VIPP 2.

36 However, as noted above, APP 6 remains complex. I consider the division between APP 6.1 and APP 6.2 unnecessary. Similarly, moving the "permitted general situations" – or exceptions – to a table (section 16A) does not assist the simplicity or lucidity of the APPs, making them more difficult to understand, and reduces the ability of States and Territories to readily adopt them with minimal amendment.

37 With respect to specific exemptions, the breadth of the exception provided by Item 6 in the table within the proposed section 16A is also of serious concern. The exception, which applies only to agencies, allows any collection, use or disclosure the agency "reasonably believes … is necessary for the entity's diplomatic or consular functions or activities". This will effectively completely exempt the Department of Foreign Affairs and Trade (**DFAT**) from the APPs. Given the existence of several other provisions including proposed APP 6.2(b), which would allow DFAT to use or disclose any personal information where the use or disclosure is required or authorised by or under an Australian law, no compelling case has been made for a further exception of such extraordinary breadth.

APP 7 – direct marketing

38 This APP provides special rules for direct marketing by private sector organisations, other than direct marketing that will be governed by the *Spam Act 2003* (Cth) or the *Do Not Call Register Act 2006* (Cth) (that is, this APP will not apply to electronic marketing or telemarketing).

39 The VIPPs do not currently deal with direct marketing separately, simply applying the other VIPPs to this type of use or disclosure. This situation will be largely unchanged under this APP.

40 As it is currently drafted, APP 7 will only apply to the private sector, unless agencies are engaging in commercial activities, as provided by the existing section 7A of the *Privacy Act*. I recommend that commercial direct marketing by public sector agencies should be covered by APP 7.

APP 8 – cross-border disclosure of personal information

41 This APP will regulate cross-border disclosures of personal information.

42 It provides that, generally, before an entity discloses personal information to an overseas recipient, it must take reasonable steps to ensure that the recipient does not breach the APPs. Under section 16C, if the overseas entity is not bound by the APPs, any act by the overseas entity that breaches an APP will be taken to have been committed by the Australian entity.

43 However, under APP 8.2 there will be a number of exceptions to these general rules, some of which, in my view, undermine the general reasoning behind the principle. APP 8.2(a) provides that if the entity "reasonably believes" that the overseas recipient is subject to a law or binding scheme that provides substantially similar protection to, or higher protection than, the APPs and the individual has access to mechanisms that enforce those protections, APP 8.1 will not apply.

44 I recommend that "reasonably believes" is removed from APP 8.2(a). If an entity seeks to rely on APP 8.2(a), it should be required to inform itself as to whether such a law or binding scheme actually exists. In the case of a complaint about APP 8, whether such a law or binding scheme exists would be determined by the Privacy Commissioner, rather than based on an entity's "reasonable" belief. One method to assist organisations in complying with APP 8.2(a), should "reasonably believes" be removed, would be for the Privacy Commissioner (or other body) to issue a list of similar laws that are substantially similar to the APPs.

45 Another exception (APP 8.2(b)) provides that where the affected individual consents to the disclosure overseas, after having been expressly informed that the entity will, as a result, not be required to take reasonable steps to ensure that the overseas recipient will comply with the APPs, APP 8.1 will not apply. As with other APPs, moving "permitted general situations" (or 'exceptions') to a table (section 16A) does not assist the simplicity or lucidity of the APPs, making them more difficult to understand, and reduces the ability of States and Territories to readily adopt them with minimal amendment.

46 If this APP was to be incorporated into Victorian law, it would largely mirror the approach the Victorian Privacy Commissioner has adopted under section 17(4) of the *Information Privacy Act*, whereby if a VIPP is incapable of being enforced against a contracted service provider (for instance, because they are outside Victoria), the outsourcing agency is held responsible. I support this view, as it ensures that the outsourcing organisation conducts "due diligence" on the overseas data recipient and takes steps to ensure that the data recipient can actually comply with the APPs, such as ensuring data security. It is my view that an organisation's consideration of whether it can or should disclose personal information should take into account the recipient's ability to comply with its legal obligations.

47 I note that APP 8 deals with "disclosure" rather than "transfer". I support this change as "disclosure" is broader than "transfer", and can mean, for instance, that a data recipient such as cloud service provider comes within the reach of APP 8 as it can technically access personal information housed on its servers. As indicated in my office's Information Sheet on cloud computing,[17] there are inherent risks with overseas data storage. There may need to be guidance issued by the Australian Privacy Commissioner as to when legitimate access of information comes within APP 8 (for example,

[17] Office of the Victorian Privacy Commissioner, Information Sheet 03.11, *Cloud Computing* (May 2011), available at http://www.privacy.vic.gov.au. My office's view is that storing information in the cloud in certain jurisdictions that do not have equivalent privacy laws could amount to a data security issue.

"disclosure" may mean *any* access to personal information, such as the illegal access of servers, even if an organisation took all reasonable steps to secure the information). Ultimately, however, I support the view that entities are accountable when disclosing, transferring or giving access to personal information to an overseas organisation.

48 However, my concern with APP 8 as currently drafted is that APP 8.2(b) gives the ability to individuals to consent to forgo any redress where their personal information is mishandled by an overseas entity. This may result in the 'bundling' of consent, where consent of the intended transfer outside Australia is provided by way of a complicated, lengthy privacy notice that will either not be read or will be easily misunderstood. I strongly support a requirement that such consent be free, express and fully informed. In its current form, APP 8.2(b) leaves open the chance that it will be abused. This potentially completely undermines any enhanced privacy protection offered by this APP.

49 Accordingly, I strongly recommend that the consent exception is either removed, or, if retained, that there be strict guidelines around its use so express consent is required. Individuals must not have consent implied or inferred by the initial or continued interaction with an entity, or where 'notice' of the intended transfer outside Australia is bundled into a lengthy privacy statement.

APP 9 – adoption, use or disclosure of government related identifiers

50 This APP provides that organisations must not adopt government-related identifiers. It does not apply to public sector agencies.

51 This is of concern, as, if incorporated into Victorian law, it would lessen the level of protection afforded by VIPP 7 to Victorians against public sector agencies adopting unique identifiers issued by other public sector agencies. Sharing of unique identifiers by public sector agencies facilitates data matching and is a very significant privacy risk, given the large amount of data that public sector agencies hold.

52 Privacy law is rooted, at least in part, in human rights law, which in turn is a response to systematic abuses of human rights often characterised by abuse of unique identifiers by government agencies. The Unique Identifiers principle addresses most directly the concerns behind the expression "just a number in a system". Privacy is part of the way a person builds and maintains his or her unique identity. As acknowledged in the second reading speech accompanying the introduction of the *Information Privacy Act* into the Victorian Parliament, to be an individual, treated as such, is an aspect of human dignity; assigning numbers to people may threaten to dehumanise them.[18]

53 The APPs should represent the highest practicable level of privacy protection. Excluding agencies from the requirements of this APP does not reflect that basic concept.

[18] Office of the Victorian Privacy Commissioner, above n 4, p 150.

APP 10 – quality of personal information

54 This APP provides that entities must take reasonable steps to ensure that personal information collected, used or disclosed is accurate, up-to-date and complete and (in the case of disclosure) relevant.

55 This largely mirrors the existing NPP 3 and VIPP 3. As such, it is welcomed.

APP 11 – security of personal information

56 This APP provides that an entity must take reasonable steps to protect personal information from misuse, interference, loss and unauthorised access, modification and disclosure. Personal information must be destroyed or de-identified if no longer needed for the purposes for which it may be used, or required to be retained for legal reasons.

57 This also largely mirrors the existing NPP 4 and VIPP 4 and is welcomed.

APP 12 – access to personal information

58 APP 12 provides for individuals' rights to access their information. Many of the existing exceptions to access rights in NPP 6 and VIPP 6 have been replicated here.

59 The right of individuals to access and correct their personal information is important for a number of reasons, as detailed by the first New Zealand Privacy Commissioner:

> Lying behind privacy legislation is a recognition of an individual's entitlement to some degree of personal autonomy. That autonomy would be illusory in many cases unless the individual can see what information is held for potential use by others. Another reason for the right of access is because of the concern that personal information to be used should be accurate and possibly the best way of ensuring such accuracy is to let the individuals see it and point out any errors. It provides some measure of accountability by agencies to the individuals whose personal information they hold and may use. Finally, an individual's right of access tends to make other aspects of the information privacy principles self-policing. Objectionable handling of personal information might tend to come to light through the individual securing access either in the hands of the agency concerned or in the hands of another agency to which the information has passed.[19]

60 I note that on 24 March 2009, the Australian Government announced as part of the reform of the *Freedom of Information Act 1982*, that the *Privacy Act* would be amended to provide for an enforceable right of access to an individual's own personal information. The language of APP 12 still does not currently reflect this.

61 In my view, an individual's right to access and correct his or her own personal information should be seen as part of the suite of privacy rights attaching to that individual, rather than part of a freedom of information scheme, the focus of which

[19] New Zealand Privacy Commissioner (Bruce Slane), *Necessary and Desirable: Privacy Act 1993 Review*, available at http://privacy.org.nz/privacy-commissioner-s-review-of-the-privacy-act.

should rightly be on the openness and transparency of government decision making. For that reason, operative access and correction provisions relating to personal information for all entities, in both public and private sectors, should form part of the APPs. Under APP 12, this is not the case.

62 If the object of the APPs is to have a single, simple set of principles to regulate the handling of personal information across the private and public sectors, then all the rules, including those concerning access and correction, should be set out as part of the APPs and be as uniform across sectors as is practicable. Access and correction rights over one's personal information are an essential component of information privacy and should be dealt with as such.

63 In New Zealand, the Privacy Commissioner and Ombudsman share the tasks in what might be called "information cases". The *Official Information Act 1982 (NZ)* originally gave everyone the right of access to their information. In 1993, the individual right of access to personal information was transferred to the New Zealand Privacy Act. Now, the Privacy Commissioner handles access requests by persons seeking their own information, and the Ombudsman handles access requests involving information other than the requester's personal information. Where an *Official Information Act* information request is refused on the grounds that it affects another person's privacy, the Ombudsman is required by the *Official Information Act* to consult with the Privacy Commissioner before forming any final views about the merits of refusing access.[20] (A similar mechanism exists in Victoria, where the Victorian Electoral Commissioner is required by section 34 of the *Electoral Act 2002 (Vic)* to consult with the Victorian Privacy Commissioner before deciding to release electoral information in the public interest, otherwise than in accordance with other authorised disclosures under that Act.)[21]

64 This type of scheme would mean that an individual's right to access and correct his or her own information and the process by which this occurs is, as far as possible, the same, regardless of whether it is held in the public or private sector. It would also enshrine an individual's right to access his or own personal information as an integral part of the right to privacy. The Bill is an opportunity for that scheme to be implemented. It is disappointing that APP 12 does not achieve this.

APP 13 – Correction of personal information

65 Again, this APP largely mirrors the existing IPP 6 and NPP 6. My only concerns again centre on the interaction with the *Freedom of Information Act*, as noted above.

[20] See New Zealand, Office of the Ombudsman, *Privacy*, Practice Guideline 4.1, available at http://www.ombudsmen.govt.nz/index.php?CID=100109.
[21] See Office of the Victorian Privacy Commissioner, *Submission to the Victorian Ombudsman on his Review of the Freedom of Information Act 1982* (Vic), August 2005, available at http://www.privacy.vic.gov.au.

Additional powers afforded to the Privacy Commissioner

66 I support the additional powers that the Bill gives to the Australian Privacy Commissioner in the Office of the Australian Information Commissioner, which include accepting and enforcing undertakings from entities, increased determination powers as part of the complaints process, and the ability to obtain civil penalties under Part VIB.

67 In particular, the ability for the Australian Privacy Commissioner to direct an agency to conduct a Privacy Impact Assessment (PIA) is welcomed. It is my hope that these powers are exercised widely, as my office has found that conducting a PIA early in a project has the ability to greatly reduce the impacts on the privacy of individuals. While there is a provision that after five years the Minister can cause a review as to whether the power to direct an agency to conduct a PIA should also apply to the private sector, I recommend removing section 33D(7) and allowing the Commissioner to direct any APP entity to conduct a PIA.

Other matters

Interaction with State and Territory Laws

68 Section 3 of the existing *Privacy Act* is retained in the Bill. This means that any State or Territory law that makes provision about interferences with privacy (including the Victorian *Information Privacy Act* and *Health Records Act*) will be preserved, if capable of operating concurrently with the *Privacy Act.*

69 While this is encouraging, as it ensures that existing protections at a State and Territory level will be preserved, it appears contrary to the recommendations of the ALRC[22] and to the Australian Government First Stage Response,[23] particularly in the area of private sector health providers.

70 In the interests of certainty, this should be clarified.

State contracts

71 A 'State contract' is defined under s 6 of the *Privacy Act* as meaning a contract:

a) to which a State, a Territory or a State or Territory authority is or was a party; and
b) under which services are to be or were to be provided to:
    i. a State or Territory authority; or
    ii. another person in connection with the performance of the functions or activities of the State or Territory authority.

72 By reason of existing sections 7B(5) and 7(1)(ee) of the *Privacy Act*, an organisation acting under such a State contract will be exempt from the APPs.

[22] ALRC, above n 1, Recommendations 3-1, 3-2.
[23] Australian Government, above n 1, p 21.

73 This is problematic, as an organisation acting under such a State contract will not necessarily be subject to State or Territory privacy laws. To begin with, neither South Australia nor Western Australia has any State privacy legislation regulating the public sector or contracted service providers in those jurisdictions. While South Australia has come a considerable way to introducing privacy legislation and is envisaged to have the legislation by the end of 2012 or shortly thereafter, Western Australia has not.

74 Even in jurisdictions which do have State or Territory privacy laws, the mere existence of a 'State contract' may not impose obligations on the organisation under State or Territory law. For example, section 17 (2) of the *Information Privacy Act* enables Victorian public sector agencies to shift liability for interferences with privacy to the contracted service provider, but this must be done under the contract, otherwise the outsourcing agency will remain liable.

75 It may therefore be possible for a contracted service provider to be exempt from the *Privacy Act* and the APPs, but not liable under State or Territory law either. While this is already the case under the existing *Privacy Act*, it is undesirable, as it may leave individuals with no redress where their privacy has been breached. The current reform of Australian privacy laws is an opportunity to redress this situation. One possible solution would be for the exemption to apply only where the organisation is subject to State or Territory privacy legislation, rather than merely a party to a State contract.

Conclusion

76 Generally, I support the changes in the Bill that give increased powers to the Office of the Australian Privacy Commissioner. Giving the Privacy Commissioner further enforcement powers will, if used effectively, increase compliance with the *Privacy Act* in both the public and private sectors.

77 The Explanatory Memorandum to the Bill states: "The Bill will reduce complexity, increase consistency and clarify rights and obligations under the Act and improve usability for entities required to comply with the Act, while continuing to protect the privacy rights of individuals."[24] As I have stated in this submission, if the APPs are intended to be used as a model for uniform legislation across States and Territories, given their complexity it will result in a lowering of privacy protection. In particular, APP 8, which deals with cross-border disclosure of personal information, has the impact to substantially lessen the privacy protection of individuals' personal information. I am disappointed that this is the case.

78 I am also concerned that in its current drafted form, the APPs are too unwieldy for individuals to understand their privacy rights. I do not think that the Bill improves usability and it is difficult to discern the consequences of such complexity. For instance, there may be additional strain on smaller organisations which, even under the existing privacy regime, may not fully appreciate their privacy obligations.

[24] *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Explanatory Memorandum, p 44.

79 It is also unfortunate that, should the Bill be enacted, the nexus between the NPPs and other privacy legislation based on the OECD principles (such as the Victorian Information Privacy Principles) is lost. As a result, the usefulness of guidance issued by my office such as the *Guidelines to the Information Privacy Principles*[25] will be sadly diminished.

80 I therefore reiterate that the more straightforward Unified Privacy Principles would better achieve the fundamental aim of the APPs. The APPs should be redrafted to reflect this aim.

81 In the era of 'big data', cloud computing and other challenges to privacy not even envisaged, Australia needs lucid and rigorous privacy legislation. The recommendations made by the ALRC in 2008 raised the promise of just such legislation. Unfortunately, the Bill in its current state does not fulfil that promise.

DR ANTHONY BENDALL
Acting Victorian Privacy Commissioner

[25] See Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, Edition 3, above n 4, which are used both nationally and internationally despite applying only to the VIPPs.