Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

Submission to the Senate Committee on Finance and Public Administration

on the

Exposure Drafts of Australian privacy amendment legislation (Australian Privacy Principles)

27 July 2010

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 Commissioner is currently on leave and has delegated all of her powers and functions to me under section 61(1) of the *Information Privacy Act 2000* (Vic).

2) While this Inquiry focuses on the Exposure Draft of the Australian Privacy Principles (APPs), as a first step in implementing the announced reforms to the *Privacy Act 1988* (Cth), the APPs have the potential to significantly impact on States and Territories (including Victoria), because of the proposed moves 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.

3) These comments are those of the Deputy Victorian Privacy Commissioner and do not necessarily represent the view of the Victorian Government.

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

[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', p. 13

[2] ALRC, op cit, Recommendation 18-1

5) The APPs, in their current form, fail to fulfil this recommendation. While in parts the APPs are expressed as high-level principles, in others the level of detail and complexity works against this aim. In a similar way, this detail and complexity means the APPs are not, as a whole, simple, clear and easy to understand and apply.For example, APP 8 (section 9), which deals with cross-border disclosure of personal information, contains within it nine separate and alternative exception clauses, many of them involving two parts. Moreover, APP 8 needs to be read in conjunction with section 20 of Part B of the Exposure Draft, which provides for the circumstances in which entities will be held responsible for the acts and practices of overseas recipients to whom they disclose personal information. This is a very complicated way in which to express the same basic concepts that were conveyed in six or seven lines in the model Unified Privacy Principles, as drafted by the ALRC.

7) In addition, a number of the exemptions included in various APPs are extremely specific to Commonwealth agencies. For example, in APP 6 (section 7), section 7(1)(f) refers to an entity's "diplomatic or consular functions", which 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. Then, 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]

Structure

8) 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.

Technological Neutrality

9) The APPs are expressed in technologically neutral language, as recommended by the ALRC.[4] This is welcome.

10) While bearing in mind the views expressed in submissions to the ALRC by Professor Roger Clarke, the Legal Aid Commission of New South Wales and Professor William Caelli that the concept of "technology neutral" legislation can in itself be problematic,[5] I support the concept of making privacy legislation "artifact neutral", in Professor Caelli's words,[6] "in that no specific manifestation of a given technology is specified."

[3] As, for example, in section 13 of the *Information Privacy Act* in relation to law enforcement agencies
[4] ALRC, op cit, Recommendation 18-1
[5] See ALRC, Discussion Paper (DP) 72, paragraphs 7.10 – 7.12, p. 344;
[6] W Caelli, Submission PR 99, 15 January 2007, cited ALRC, DP 72, paragraph 7.12, p. 344;

11) Should a specific future technology develop that is so privacy intrusive as to require regulation, it will be the job of governments and parliaments, in consultation with Privacy Commissioners, to enact specific future legislation to deal with this. Otherwise, privacy principles like the APPs should be expressed in such a way as to effectively deal with collection, storage, access to, correction, use and disclosure of personal information, regardless of the specific technology used in each of these processes.

The Principles

APP 1 – open and transparent management of personal information

12) This APP 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 entity (public sector agency or private sector organisation) complies with the APPs and enable 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, if it is practicable to specify them.

13) This is considerably more prescriptive and detailed than the existing National Privacy Principle (NPP) 5 in the *Privacy Act* 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

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

APP 2 – anonymity and pseudonymity

15) 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. I agree with the ALRC's view that the inclusion of this principle will maximise an individual's control over his or her personal information whilst interacting with government.

16) VIPP 8 currently gives Victorians the option of transacting anonymously with Victorian public sector organisations wherever it is lawful and practicable to do so.[7]

17) 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

[7] Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, Edition 2, September 2006, at paragraphs 8:4 to 8:24., pp 145 to 149, available at www.privacy.vic.gov.au/privacy/web.nsf/content/guidelines

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.

18) 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

19) This APP 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).

20) I am concerned by the use of the terms "reasonably necessary" and "or directly related to". 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.

21) 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"[8] and consequently 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 proportionate[9] or what may involve "close scrutiny, congruent with a search for 'compelling justification'".[10]

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.

[8] *Ng v Department of Education* [2005] VCAT 1054 at para 77.
[9] *Mulholland v Australian Electoral Commission* [2004] HCA 41 at 33-39 and 249-251.
[10] *Mulholland v Australian Electoral Commission* [2004] HCA 41 at 39-40.

23) I would support a narrower drafting of this principle 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", IPP 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.[11]

24) Moreover, some of the exceptions that relate solely to Commonwealth agencies are 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 (see above).

25) Section 4(5) 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.

26) 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 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.[12]

27) 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.[13]

28) 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;

[11] Office of the Victorian Privacy Commissioner, op.cit., at paras 10.32 to 10.35;
[12] Ibid, at para 1:92, p 38.
[13] Ibid, para 1:93, p 38.

- 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).[14]

29) 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.[15]

30) 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.[16]

APP 4 – receiving unsolicited information

31) This APP 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 APP 5 to 13. If not, it must destroy or effectively de-identify that information.

32) While the VIPPs do not currently explicitly deal with this situation, as VIPP 1 makes no distinction between solicited and unsolicited information, it reflects the interpretation and approach adopted by the Victorian Privacy Commissioner and is welcomed.[17]

APP 5 – notification of the collection of personal information

33) 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 it 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.

34) I strongly support this APP. 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

[14] Office of the Australian Privacy Commissioner, *Guidelines to the National Privacy Principles,* (2001) p 31-2.
[15] Office of the Victorian Privacy Commissioner, op.cit., KC:90, p 23.
[16] See, for example, *Seven Network (Operation) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637.
[17] See OVPC, op cit, paras 1:13 to 1:18, pp 27-28

accessing) their information.[18] 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.

35) 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' privacy principle, like APP 1.[19]

APP 6 – use or disclosure of personal information

36) This APP 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 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.

37) However, some other exceptions to the general rule are of concern. Sections 7(2)(f) and (g) relate solely to Commonwealth agencies and as such are problematic when expressly included in the APP itself. This reduces the simplicity, lucidity and "high-level" nature of the APPs. As well as making them more difficult to understand, it also reduces the ability of States and Territories to readily adopt them with minimal amendment (see above).

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. As it is currently drafted, it 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*. Coverage of commercial direct marketing by public sector agencies is welcomed.

[18] OVPC, op.cit, para 1: 61, p 34.
[19] Ibid, para 1: 72, p 35.

APP 8 – cross-border disclosure of personal information

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

41) 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. 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.

42) However, there will be a number of exceptions to these general rules. One is where the overseas recipient is subject to a law or binding scheme that provides substantially similar, or higher protection, than the Australian Privacy Principles and the individual has access to mechanisms that enforce those protections. Another exception is 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.

43) There are other exceptions which apply solely to Commonwealth agencies. As with other APPs (see above), such exceptions are problematic when expressly included in the APP itself. This reduces the simplicity, lucidity and "high-level" nature of the APPs. As well as making them more difficult to understand, it also reduces the ability of States and Territories to readily adopt them with minimal amendment

44) 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.

45) However, the ability of individuals to consent to forgoing any redress where their personal information is mishandled by an overseas entity is of concern. If the "consent exception" is to remain, it needs to be tightly controlled, so that individuals cannot have implied consent inferred by the initial or continued interaction with an entity, or where 'notice' of the intended transfer outside Australia is provided by way of a complicated, lengthy privacy notice that will either not be read or easily misunderstood. I strongly support a requirement that such consent be free, express and fully informed.

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

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

47) 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.

48) 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 '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 indentify. 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.[20]

49) 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.

IPP 10 – quality of personal information

50) 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.

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

IPP 11 – security of personal information

52) 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.

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

IPP 12 – access to personal information

54) This APP 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.

55) The right of individuals to access and correct their personal information is important for a number of reasons, as detailed by the 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*

[20] Guidelines, 7:2 and 7:3, p 135.

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.[21]

56) I note that 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 does not currently reflect this. The Companion Guide indicates that this is due to a number of technical issues which will be resolved subsequently. It is important that they are.

57) 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.

58) 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.[22] (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.)[23]

---

[21] New Zealand Privacy Commissioner (Bruce Slane), *Necessary and Desirable: Privacy Act 1993 Review*, Report of the Privacy Commissioner

[22]See New Zealand, Office of the Ombudsman, *Privacy,* Practice guideline 4.1; New Zealand, Office of the Privacy Commissioner, *The Roles of the Ombudsman and the Privacy Commissioner,* Fact sheet 11;

[23] 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/dir100/priweb.nsf/content/5D37ECB57A98BDA7CA256C4D0019E8AD?OpenDocument, accessed 5 December 2007;

59) 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.

60) I look forward to the technical issues noted in the Companion Guide being resolved in such a way as to allow this to also occur at the Australian Commonwealth level. This will be facilitated by the fact that, after 1 November 2010, the ultimate decision maker under both the *Freedom of Information Act* and the *Privacy Act* will be the Australian Information Commissioner.

IPP 13 – Correction of personal information

61) 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* which I am confident will be resolved.

Other matters

Interaction with State and Territory Laws

62) The Companion Guide indicates that section 3 of the existing *Privacy Act* will be replicated in the new *Privacy Act*. This will mean 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.*

63) 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[24] and to the Australian Government First Stage Response[25], particularly in the area of private sector health providers.

64) In the interests of certainty, this should be clarified.

State contracts

65) Section 15 of the Exposure Draft defines 'State contract' 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.

66) 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.

[24] ALRC, op cit, Recommendations 3-1, 3-2
[25] Australian Government, op cit, p 21

67) 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.

68) 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.

69) 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

70) In summary, the Exposure Draft of the APPs largely embodies the concepts recommended by the ALRC and accepted by the Australian Government. However, some anomalies remain, as outlined above. These should be resolved.

71) Moreover, the current drafting of the APPs works against the simplification and harmonisation which was the core recommendation of the ALRC. The APPs should be redrafted in order to achieve this fundamental objective.

DR ANTHONY BENDALL
Deputy Victorian Privacy Commissioner