NSW GOVERNMENT | Justice & Attorney General

Submission to the Senate Finance and Public Administration Committee on the Australian Privacy Principles Exposure Draft

December 2010

Background

The Senate Finance and Public Administration Committee is holding an inquiry into an exposure draft of the proposed new *Australian Privacy Principles* (**draft Principles**).

The Australian Law Reform Commission's (**ALRC**) Report 108, *For Your Information: Australian Privacy Law and Practice*[1] was released in August 2008. In its first-stage response to the ALRC's Report 108, the Australian Government accepted two of the ALRC's recommendations regarding national consistency in privacy regulation.[2] It also stated that there are clear benefits of nationally consistent privacy regulation in the private sector, including the health sector, and that that it will work with State and Territory counterparts to progress privacy reforms.[3]

Given the potential for greater national consistency of privacy laws, it is important that States and Territories contribute to the discussion about the content of the draft Principles.

This submission addresses the content of, and the policy expressed by, the draft Principles. It does so in light of the ALRC's recommendations and those of the New South Wales Law Reform Commission (**NSW LRC**) in its August 2009 Report 123, *Privacy Principles*.[4] It does not comment on the extent to which the draft Principles should apply to NSW at any future date nor does it set out the final position of the NSW Government on these issues.

Health Information

It is not clear whether the APPs are intended to apply to health information and health care providers. The Companion Guide notes that there will be further public consultation on specific privacy protection principles relating to health. However, the definition of sensitive information in the Exposure Draft includes "health information"

---

[1] Australian Law Reform Commission, *For Your Information; Australian Privacy Law and Practice*, Report 108 (2008) (ALRC Report 108).
[2] ALRC Report 108 Recommendations 3.1 and 3.2.
[3] Australian Government, *Enhancing National Privacy Protection; Australian Government First Stage Response to the Australian Law reform Commission Report 108 'For Your Information: Australian Privacy Law and Practice"*, October 2009 at 21.
[4] New South Wales Law Reform Commission, *Privacy Principles,* Report 123 (2009) (NSW LRC Report 123).

which implies that healthcare providers must comply with the APPs when collecting, using and disclosing health information. Assuming that the APPs apply to health information and healthcare providers, specific comments have been provided from a health perspective in relation to APP 3, APP 6 and the definitions.

APP1 - Open and transparent management of personal information

- The requirement that an entity take reasonable steps to make its privacy policy electronically available, as proposed by the ALRC[5], has not been included in APP1. In the interests of transparency and accountability, APP1 could explicitly state that entities should take reasonable steps to make the policy available electronically. In practice, this will most likely result in policies being posted on the websites of entities that have them. This is likely to be the first place members of the public will look for privacy policies and it may be appropriate to make explicit the requirement to make them available in this manner.

- APP1 could be drafted to emphasise the policy intent that entities should plan how to handle personal information *before* they collect it. That is, the temporal element could be clearer. This may be achieved with a minor adjustment in the language, for example, by re-titling the heading to APP1(2) "*Planning* for compliance with the Australian Privacy Principles".

- It may be preferable for privacy policies to contain not only "the purposes for which the entity ... discloses personal information" but also some description of the individuals or entities who are most likely to receive it. This is crucial in terms of giving members of the public a real picture of how personal information is handled and to answer the question: "who are they giving it to?"

  The ALRC did not think this necessary if entities were required to set out a general description of disclosure practices.[6] The APP1(4) arguably does not require this as it states only that the *purposes* of disclosure be described. This is a different question to the identity of persons or entities to whom disclosures will likely be made. As presently drafted, an entity might interpret APP1(4) in a manner that led to no description of the latter.

  The ALRC also considered that the obligation under the notification principle (now in APP5(f)) to provide information about usual disclosures made it unnecessary to require this in a privacy policy.[7] However, notifying individuals in this manner is different to including such matters in a privacy policy which benefits the public at large. Individuals may wish to peruse a privacy policy before entering into any interaction with an entity and before the requirement under the notification principle applies. A requirement to describe the persons to whom disclosures are usually made would complement, not duplicate, the inclusion of this matter in the notification principle.[8] A requirement of this sort is unlikely to impose any significant burden on entities.

---

[5] ALRC Report 108 Recommendation 24-2.
[6] ALRC Report 108 at 820.
[7] ALRC Report 108 at 821.
[8] See ALRC Report 108 at [24.51] – [24.52] in relation to other matters to be included in privacy policies.

APP2 – Anonymity and pseudonymity

- As presently phrased, APP2 could be read to require *either* the option of anonymity *or* pseudonymity. The ALRC recommended that both options should be available. The drafting of the principle could make this clear, for example, by replacing the term "or" with the term "and". There could be an exception from the requirement to provide both these options if one is not practicable, perhaps through an amendment to APP2(2). For example, pseudonymity may be practicable where anonymity is not, and in this case an entity should only be required to make the former available.

- In addition, APP2 could be drafted as recommended by the ALRC, to make clear that the onus of providing the clear option of anonymity or pseudonymity lies on entities.[9] As presently drafted, APP2 is expressed in the passive voice and does not make this clear.

- The ALRC's view was that the qualifications to the principle relating to lawfulness and practicability would be sufficient to address most agencies' concerns about the operation of this principle. As suggested by the ALRC, agencies should be able to gain further guidance about this principle from guidelines issued by the Office of the Australian Information Commissioner.[10]

  Guidelines on the circumstances in which compliance is to be considered impracticable under APP2 should set out matters to be considered in deciding whether compliance is practicable. They could make clear, for example, as suggested by the ALRC, that anonymity or pseudonymity generally will not be lawful in the provision of government benefits. It will be important that States are consulted on the content of any such Guidelines.

APP3 - Collection of solicited personal information.

- The NSW Law Reform Commission recommended that an entity should be able to collect personal information about an individual from a third party if the individual consents, as is currently the case under s9 of the *Privacy and Personal Information Protection Act 1998* (NSW) (**PPIPA**).[11] APP3 does not accord with this approach.

  The NSW LRC's proposed "consent" exception, as the Commission pointed out, gives individuals autonomy about how their personal information may be collected.[12] An individual may prefer to have an entity gather their personal information from third parties rather than having to keep interacting with the entity. This may be an important matter of convenience for individuals as well as entities. The NSW LRC's view was that:

---

[9] ALRC Report 108 at [20.64].
[10] ALRC Report 108 [20.44].
[11] NSW LRC Report 123 at [2.46].
[12] NSW LRC Report 123 at [2.46].

"...the law should sanction such collection, even if it would be reasonable or practicable for the agency or organisation to collect the information from the individual."[13]

The NSW Minister for Housing, in her submission to the NSW LRC, gave an example of where this exception should apply. She stated that her Department may need to collect information from a medical practitioner about the mental health of an applicant for priority housing. An application form for housing could provide for the consent of the individual to the Department obtaining information about them from specified third parties.[14] As the Commission pointed out, it is possible that in such a case, it might not be unreasonable or impracticable to obtain the information from the individual in question. Thus, as presently drafted APP3 might not authorise the Department to obtain such information from the medical practitioner.

- The ALRC did not directly address the question of whether there should be an exception of "consent" to the collection principle. However, the ALRC noted that, generally speaking, the arguments against obtaining information from third parties are that individuals will not have the ongoing opportunity to refuse to provide their information, and that there is a risk that information obtained from third parties will not be up-to-date, complete or accurate.[15] Any such risk may be mitigated by the fact that entities may treat third-party information with greater caution, but there is no guarantee of this. It is also arguable that where individuals themselves choose to rely on third parties to provide their information, they impliedly accept these risks, but individuals may not have turned their mind to them.

- There are difficulties arising from the concept of consent. Ideally such consent is voluntary, informed and express. However, the application of the concept is far from simple. For example, "consent" may be affected by social disadvantage such as illiteracy or a lack of knowledge about the right to refuse to give information.[16] There is also the question of "bundled consent", that is, where an entity bundles "multiple requests for an individuals' consent to a wide range of uses and disclosures of personal information, without giving the individuals the option of selecting to which uses and disclosures he or she agrees"[17]. The NSW LRC did not address these questions in recommending the consent exception.

- The draft Principles define consent to include express or implied consent (s15). If a "consent" exception is to be implemented, it may be appropriate to limit it to cases of express consent. In the example given above, for example, the express consent would come from the housing application form, specifying the parties from whom information is to be collected and for what specific purpose. Alternatively, the concerns about the concept of "consent" may be addressed

---

[13] NSW LRC Report 123 at [2.46].
[14] NSW LRC Report 123 at [2.41].
[15] ALRC Report 108 at [21.20].
[16] See ALRC Report 108 at [19.37].
[17] ALRC Report 108 at [19.25].

through guidelines issued by the Office of the Privacy Commissioner, as recommended by the ALRC.[18]

- It is submitted that it would be preferable to allow entities to collect information from third parties where an individual gives their express consent. While there are some risks in relation to the nature of the consent and the accuracy and completeness of the information, individuals should be free to choose to have their information collected from third parties where they do not wish to provide the information themselves.

- *Health information and APP3*

  In the area of health, health practitioners will routinely collect health and medical information about individuals without their consent and in circumstances where it is not practicable to obtain that individual's consent. This primarily happens in the context of providing care to a patient, and as part of that care, a family history of the patient is taken. In order to provide appropriate care to the patient, the health practitioner will need to know the medical history of the patient's family members.

  As APP3 is currently drafted, there is no current exception to the collection of sensitive information that would allow this to occur. A health practitioner will not have the patient's family member's consent (so APP3(2) will not apply) and, in most circumstances, the information collected about a patient's family members will not be necessary to lessen or prevent a serious threat to life, health or safety (so APP(3)(b) will not apply).

  It is imperative that health practitioners can continue to take a patient's family history without having to seek the consent of each family member to collect health information about that family member. APP3 should be amended to allow this to occur.

APP4 – Receiving unsolicited personal information

As presently drafted, APP4 requires that all unsolicited information be assessed to determine if the information *could* have been collected under APP3, and if the answer is yes then APPs 5-13 must be complied with. The ALRC's Recommendation 21-3, if implemented, would have allowed an agency, if it did not wish to retain unsolicited information, to destroy it without having to decide whether it could have collected the information under APP3. Recommendation 21-3 would also have allowed the agency to destroy the information if it decided that it could have lawfully collected it, without the need to then comply with other privacy principles. It may be preferable to give agencies the option of destroying unsolicited information as the ALRC proposed.

APP5 – Notification of the collection of personal information

No comment.

---

[18] ALRC Report 108, Recommendation 19-1.

APP6 – Use or disclosure of personal information

- In relation to APP6(2)(a), the ALRC's Recommendation 25-2 has been amended to include a requirement that the "affected individual would reasonably expect the entity to use or disclose the information for the secondary purpose". The NSW LRC recommended that the ALRC's Recommendation 25-2 be amended in a different manner, by including a requirement that "the agency has no reason to believe that the individual would object".[19]

  The NSW LRC's approach caters for the situation where an individual does in fact object to the use or disclosure of their information for a secondary purpose. It appears that the LRC's approach would require an agency not to use or disclose personal information for a secondary purpose in the face of an objection from the relevant individual, whether that objection was reasonable or unreasonable. In contrast, APP6 as currently drafted appears to allow an agency to use or disclose personal information for a secondary purpose even in the face of an objection from the individual (reasonable or unreasonable).

  The reasonable expectation test in APP6 is a useful one however APP6 could also be amended so that if an individual objects to their information being used for a secondary purpose, the information cannot be so used. There is a question whether such objections should meet a test of "reasonableness" or not. On the one hand, there is an argument that any objection should prevent disclosure for secondary purposes, whether the objection is reasonable or not. On this view, agencies should not be able to treat personal information as a resource to be drawn on for secondary purposes in the face of objections from the individual to whom the information relates. On the other hand, there may be an argument that in some circumstances agencies *should* be able to disclose or use personal information for a secondary purpose where an individual objects but that objection is unreasonable.

- It is noted that no "research" exception to the use and disclosure principle has been included in APP6, contrary to the ALRC's Recommendations 65-2, 65-4 and 65-9. Presumably such an exception will be located elsewhere in any new privacy legislation, since the Government accepted these recommendations in its First Stage Response to the ALRC's Report.[20] If so, a note should be included at the end of APP6 to direct readers to this exception.

- *Health information and APP6*

  As currently drafted, APP6 has a number of problems associated with the use and disclosure of health information.

  APP6(2)(d) allows an entity to use or disclose personal information, including health information, if the entity suspects that unlawful activity or serious misconduct, that relates to the entity's functions is being engaged in and the

[19] NSW LRC Report 123, Recommendation 5.
[20] Australian Government, *Enhancing National Privacy Protection; Australian Government First Stage Response to the Australian Law reform Commission Report 108 'For Your Information: Australian Privacy Law and Practice"*, October 2009 at 53.

entity believes the use/disclosure of the information is necessary for the entity to take appropriate action. APP6(2)(d) is only focused on unlawful activity or serious misconduct of the entity. It does not extend to a situation where an entity suspects that unlawful activity or serious misconduct by another person or entity is occurring.

In the case of suspected unlawful activity by a person other than the entity, APP6(2)(e) will apply. However, in the case of suspected serious misconduct, such as professional misconduct by a person other than then entity, there is no means by which the entity can use/disclose the information. This is of particular concern in respect of health information. A health practitioner may come across information, either from a patient or from their own observations, that another practitioner is engaging in professional misconduct or unsatisfactory professional conduct. In these circumstances, the APPs should allow the practitioner to report their concerns to the appropriate body. While in some cases, reporting of such concerns will fall within APP6(2)(b) (authorised or required under an Australian law), APP6(2)(b) will not apply in all cases where an entity suspects another person or entity is engaging in professional misconduct or unsatisfactory professional conduct.

APP6 should be amended in order to ensure that entities can report their concerns, to an appropriate body, about suspected professional misconduct or unsatisfactory professional conduct engaged in by another entity or person.

There are also a number of missing essential permitted uses and disclosures of health information in APP6:

- Research. As noted above, APP6 does not allow personal information, including health information, to be used/ disclosed for the purpose of research. This is allowed under the current NPPs (as well as under provisions in State privacy legislation). A "research" exception to the use and disclosure principle is particularly important in the field of health where research is a necessary component of health.
- Training/Management of health services. The current NPPs allow health information to be used/ disclosed for the purpose of the management, funding and monitoring of health services. APP6 does not contain any equivalent provision and this should be rectified. It is essential that healthcare providers can use/disclose health information for the purpose of the management (including training), funding and monitoring of health services.

One other issue of concern is that APP6(2)(g) allows an entity to use/disclose personal information if the entity reasonably believes the information is reasonably necessary to assist any entity, body or person to locate a missing person (and the entity complies with relevant privacy rules). The inclusion of a missing person exception is welcome. However, as it is currently drafted, APP6(2)(g) is too broad and unduly impacts on a person's privacy.

APP6(2)(g) would allow information, including sensitive health information, to be disclosed to any person or body to locate a missing person. This would include not just the Police, or other investigative agency, but the missing person's family

or a private investigator. It is not considered appropriate to allow personal information about a missing person to be disclosed to any person other than the Police (or other investigative agency). A missing person might have gone missing for a number of reasons and may not want to be found by their family or other persons, for example persons leaving abusive relationships who do not want any contact with their abuser and who will not want their abuser to be given any information about them. APP6(2)(g) should be amended to only allow information to be disclosed to the Police for the purpose of locating a missing person. An entity should not be able to disclose personal information to bodies or persons other than the Police, even in accordance with privacy rules.

APP7 – Direct marketing

The subtitle to APP7(3) is presently confusing in that it refers to "personal information collected from another person etc" but then subss(3)(a)(i) deals with the information collected from the individual concerned.

APP8 – Cross border disclosures of personal information

- The ALRC recommended that entities that transfer personal information to overseas recipients remain accountable for that personal information, and for interferences with privacy by overseas recipients, subject to some exceptions.[21] APP8 itself does not embody this principle, requiring only that such entities "take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the [APPs]." However, s20 of the Exposure Draft does embody the "accountability" principle.

  For clarity, the accountability principle could be embodied in the relevant APP and not in a separate section of the Act. At the least, a note could be included following APP8 to indicate that the accountability principle applies and stating its location. At present, there is a risk that entities or individuals will turn to the legislation and assume that APP8 is exhaustive in relation to cross-border transfers. It could appear that the only obligation on entities is to take reasonable steps to ensure that the overseas recipient does not breach the APPs, which provides a far more limited safeguard than the accountability principle that appears in s20.

- *Reasonable belief exception*

  The ALRC recommended that entities transferring personal information overseas should not be accountable for the information if the entity "reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model Unified Privacy Principles".[22] However, the ALRC also recommended that the Australian Government publish and maintain a list of overseas laws and binding schemes that effectively uphold principles for the fair

[21] ALRC Report 108, Recommendation 31-2, 31-3.
[22] ALRC Report 108, Recommendation 31-2.

handling of personal information that are substantially similar to the Unified Privacy Principles.[23]

The NSW LRC's view is that, if such a list is published, there is no need for the reasonable belief test.[24] Such a list could include not only laws but also "binding schemes" such as inter-governmental agreements or effective self-regulatory schemes.[25] There is a question about the circumstances in which an entity could hold the necessary 'reasonable belief' in relation to an entity in a jurisdiction not on the list. It is conceivable that a jurisdiction with adequate protection might not be on the list due to delays in maintaining the list. In such circumstances, the reasonable belief test could provide a safety net for entities. However, provided the list is effectively created and maintained, in the vast majority of cases a belief is unlikely to be 'reasonable' in relation to an entity in a non-listed jurisdiction. Alternatively, a belief may be reasonable, based on the information available to an entity, but it may be ill informed and incorrect. The NSW LRC's Recommendation 14, to remove the "reasonable belief" exception in favour of the "listed jurisdiction" approach, may be worth further consideration.

There is also an argument that the test should not be restricted to whether another jurisdiction's protections are "substantially similar" to the APPs but should also cover jurisdictions where a different approach is taken but where the privacy protection achieved is the same or greater than that achieved by the APPs.[26]

APP9 – Adoption, use or disclosure of government related identifiers

The APP9 definition of "identifier" excludes biometric information. This approach is contrary to the recommendations of the ALRC[27] and the NSWLRC[28] and should be further considered. This was apparently done on the basis that "[t]he collection of such information by organisations will not result in the privacy risks that the 'identifiers' principle is intended to address, such as the risk of an identifier becoming widely held and applied to facilitate extensive data-matching or data-linking."[29] However, it is possible that, especially with advances in technology, biometric data may be used in the same way as a set of numbers in that it may be passed to various entities and linked to certain information.

APP10 – Quality of personal information

No comment.

---

[23] ALRC Report 108, Recommendation 31-6.
[24] NSW LRC Report 123 at [11.52].
[25] NSW LRC Report 123 at [11.56].
[26] See NSW LRC Report at [11.49] and Recommendation 14.
[27] ALRC Report 108, Recommendation 30-3.
[28] NSW LRC Report 123 at [10.32].
[29] Australian Government, *Enhancing National Privacy Protection; Australian Government First Stage Response to the Australian Law reform Commission Report 108 'For Your Information: Australian Privacy Law and Practice"*, October 2009 at 74.

APP11 – Security of personal information

Section 12(d) of PPIPA provides:

> *12 Retention and security of personal information*
>
> *A public sector agency that holds personal information must ensure:*
> ...
> *(d) that, if it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency is done to prevent unauthorised use or disclosure of the information.*

APP 11 imposes no such requirement on agencies. However, s95B of the *Privacy Act 1988* (Cth) imposes such a requirement on Commonwealth agencies. In practice, many contractors will be subject to APP11 at any rate, since it applies to organisations. However, APP11 will not apply to small business contractors since they are excluded from the definition of "organisation".[30]

Consideration should be given to replicating the requirement imposed on agencies by s12(d) of PPIPA and s95B of the *Privacy Act* in any model privacy laws if it is not to be provided for by the APPs.

APP12 – Access to personal information

No comment.

APP13 – Correction of personal information

No comment.

Section 15 Definitions

- The definition of "sensitive information" currently includes "criminal history". The meaning of the term "criminal history" is not entirely clear but, as the NSW LRC pointed out, it may not extend to information about arrests and charges that do not result in a formal criminal record.[31] Such information is also very sensitive in nature and consideration should be given to including it in the definition. Further consideration should be given to including biometric data in the definition of "sensitive information".

- It is not clear from the definition of "order of court of tribunal" in clause 15 whether the definition extends to courts and tribunals of the States and Territories.

- The term "health information" (in the definition of "sensitive information" in clause 15) is not defined and it is not clear whether the current definition in the Privacy Act 1988 will be used.

- The definition of a "State of Territory authority" in clause 15 includes at (e):

---

[30] s17 Exposure Draft of the Australian Privacy Principles.
[31] NSW LRC Report 123 at [5.80].

a person who holds or performs the duties of:

i) An office established by or under a law of a State or Territory; or

ii) An appointment made under such a law;

other than the head of a Department of a State or Territory (however described).

Subclause (f) of the definition includes within the definition of a "State or Territory authority":

a person holding or performing the duties of an appointment made, otherwise than under a law of a State or Territory, by:

i) a Governor of a State; or

ii) the Australian Capital Territory Executive; or

iii) the Administrator of the Northern Territory; or

iv) the Administrator of Norfolk Island; or

v) a State or Territory Minister; or

vi) a person holding an executive office mentioned in section 12 of the Norfolk Island Act 1979 .

This definition is the same as is used in the current Privacy Act 1988. However, as is currently drafted, it appears that a head of a Department of a State or Territory who is appointed under a law of a State or Territory, rather than appointed under a State or Territory's Minister prerogative, is not considered to be a "State or Territory authority". This is problematic in NSW where heads of Departments are appointed under the Public Sector Employment and Management Act 2002.

There is no discernable reason why a Department head's inclusion in the definition of a "State or Territory authority" should be dependent on the manner in which the Department head is appointed. The recently commenced Healthcare Identifier Act 2010 takes into account the fact that Department heads of a State or Territory, however an appointment is made, should be considered to be part of a State or Territory "public body". It does this by including in the definition of "public body" a "State or Territory authority" (within the meaning of the Privacy Act) as well as "the head (however described) of a Department of State of the State or Territory" (section 5 of the Healthcare Identifier Act 2010).

The definition of a "State of Territory authority" in clause 15 should be amended to make clear that the definition includes the Department Head of a State or Territory, however the appointment is made.

General comment

The numbering of Australian Privacy Principle (APP) 1 as section 2 and APP2 as section 3, and so on, is not ideal and may lead to errors in referencing. A numbering system referring only to the number of the privacy principle in question could be developed, or alternatively, section numbers only could be used, as in PPIPA, Part 2, Div 1.