Exposure Draft of the Australian Privacy Principles

To: Senate Finance and Public Administration Committee

19 August 2010

Queries regarding this submission should be directed to:
Contact persons
Ph
Email

Table of Contents

Introduction

The Law Institute of Victoria (LIV) welcomes the opportunity to provide comments on the Australian Privacy Principles (APPs) Exposure Draft (the Draft) and is grateful that the Senate Finance and Public Administration Committee has extended time for submission of comments.

The LIV is Victoria's peak representative body for lawyers and those who work with them in the legal sector, representing over 14,500 members. The LIV's Administrative Review and Constitutional Law Committee is made up of legal practitioners experienced in administrative and constitutional law. Committee members have a special interest in Australia's privacy laws and how they impact on the rights and obligations of individuals. Many also have experience representing applicants under Australia's current privacy laws and therefore have insight into how changes to privacy laws can cause administrative law repercussions for government agencies responsible for the creation and implementation of these laws.

General comments

Rapid advances in information, communication, storage, surveillance and other relevant technologies have significant implications for individual privacy. Persons have a right not to have their privacy unlawfully or arbitrarily interfered with (protected, for example, in Article 17 of the International Covenant on Civil and Political Rights). The LIV believes that the protection of an individual's privacy is fundamental to their human dignity and is central to many other human rights such as the right of freedom of association, movement and expression.

The LIV therefore welcomes implementation of recommendation 18 of the Australian Law Reform Commission report *For Your Information: Australian Privacy Law and Practice* (the ALRC report) in the Draft. Recommendation 18 provides that the privacy principles in the *Privacy Act* 1988 (Cth) should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles and drafted so that they are: generally expressed as high-level principles; technology neutral; simple, clear and easy to understand and apply; and impose reasonable obligations on agencies and organisations. We urge the government to implement the remaining ALRC recommendations as soon as possible to ensure that Australia is able to adequately protect the privacy of its citizens and residents.

The LIV is concerned, however, that the Draft does not address the issue of ownership and control of information about a person. The LIV believes that proper consideration should be given to data ownership and control because entities are more likely to impinge upon individual rights if data is not collected, stored and used in an appropriate way.

The LIV suggests that the APPs should specifically address the issue of who owns personal information. The APPs currently defines personal information (and sensitive information) to include both information and opinions about a person (see cl 15). The LIV considers that a distinction should be drawn in the APPs between information (which might include information such as identity information, biometric information, date of birth, name and address) which we propose be called "primary personal information", and opinions held about an individual, which we propose be called "secondary personal information". The LIV considers that individuals should be able to retain ownership of primary personal information about them. Further, the LIV submits that the APPs should provide that when requested to do so, entities should be required to destroy primary personal information held about an individual (subject to any statutory rights of agencies to collect or retain information).

The LIV is concerned about numbering in the Draft and suggests that for consistency and ease of reference, each APP be numbered the same as the section or clause number. For the purposes of this submission, the LIV refers in Part A to each APP together with its subclause (eg APP 1(2)) and does not refer to the clause number in the Draft.

The LIV respectfully submits that the current Draft would be significantly improved with the enactment of changes set out below.

Part A – Australian Privacy Principles

APP 1: open and transparent management of personal information

APP 1(2) requires an entity to "take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities" that will ensure that the entity complies with the APP and will enable the entity to deal with complaints from individuals about compliance with the APP. It is the LIV's view that this statement should be amended to read "implement *and review* practices" as this would be consistent with APP 1(3), which requires entities to have "up-to-date policy" on the management of personal information.

The Draft is also silent on what constitutes "up-to-date policy" as required to be prepared by entities under APP 1(3). The LIV suggests that guidance notes should be developed by the Privacy Commissioner to specify how often entities should conduct reviews as this would assist entities with compliance in practice.

APP 2: anonymity and pseudonymity

APP 2(1) provides that individuals must have the option of not identifying themselves when dealing with an entity, unless the entity is required or authorised by law to deal only with individuals who have identified themselves (APP 2(2)(a)) or it is impracticable for an entity to deal with individuals who have not identified themselves (APP 2 (2)(b)).

The LIV is concerned that the scope of APP 2 (2)(b) is overly broad, and may enable entities to circumvent compliance with APP 2(1). We therefore recommend that "impracticable" be defined in guidance notes with a view to ensuring that practicability is relevant to the service or goods that the individual seeks to access.

The LIV notes that APP 2 does not address how an individual might establish that it is not impracticable for an entity to deal with them on an anonymous basis. The LIV suggests that transparency would be improved if entities wishing to rely on APP 2(2)(b) and who claim that it is impracticable to deal with individuals who have not identified themselves, be required to address this issue in their privacy policy or in a specific statement to individuals when personal information is sought.

The LIV suggests that APP 5 be amended so that at the time of collection of information, entities are required to notify the individual about their right not to provide identity information. This could be achieved by including this information in the list of matters under APP 5(2). Entities could also be required to include a statement about anonymity in their privacy policy. This could be achieved by way of amendment to the list of information that must be contained in a privacy policy in APP 1(4).

APP 3: collection of solicited personal information

<u>Test of "reasonably necessary…to one or more of the entity's functions or activities"</u>

Under APP 3(1), an entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

The LIV notes that the construction of APP 3(1) allows multi-function entities to request personal information that is not directly related to the goods or services actually requested by an individual, so long as the information is reasonably necessary for one or more of the entity's functions. The LIV is concerned that APP 3(1) might enable entities to make the provision of goods and services

conditional upon irrelevant and potentially unnecessary personal information being provided by an individual. We note that this situation may be alleviated by APP 2, which provides that individuals must have the option of not identifying themselves when dealing with an entity. However, we note that individuals must be made aware of their right to deal with the entity anonymously and refer to our proposal above to amend APP 5(2) and APP 1(4) to achieve this.

The Companion Guide to the Draft states that the test of "reasonably necessary…to one or more of the entity's functions or activities" in APP 3 is intended to be interpreted objectively and in a practical way. The LIV considers, however, that this is a unilateral test that focuses only on the entity's functions and not on the individual's reasons for disclosing personal information or dealing with the entity. The test is broad and permits the collection of personal information for any of the entity's purposes, even if the individual has transacted in respect of a confined, limited function or activity. The LIV recommends that this test, wherever appearing, should be amended to "reasonably necessary for the function or activity in which the individual is engaging" or similar.

We note that the broad test of "reasonably necessary" for collection of information is subject to APP 6 in respect of use of that information once collected and we refer further to our comments below.

Consent

APP 3(2) provides that an entity must not collect sensitive information about an individual unless information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities and the individual consents to the collection of information. Consent is defined in cl 15 to mean express consent or implied consent. Clause 15 defines sensitive information to mean personal information that is information or an opinion about an individual's: racial or ethnic origin; political opinions; membership of a political association; religious beliefs or affiliations; philosophical beliefs; membership of a professional or trade association; membership of a trade union; sexual orientation or practices; criminal record; or health, genetic or biometric information about an individual.

If goods or services are withheld unless an individual "consents" to a secondary use or disclosure, where that use or disclosure is not related to, or necessary for, the primary use or disclosure, can it really be called "consent"? We reiterate our comments above that this situation might be alleviated by APP 2, which provides that individuals must have the option of not identifying themselves when dealing with an entity, and our suggestions about ensuring that individuals are notified about this.

The LIV submits that individuals cannot consent to the collection of sensitive personal information where consent is obtained in a coercive or unreasonable way. To this end, we submit that the Draft's definition of consent requires further development and clarification because it does not preclude consent from being obtained unreasonably or in a way that undermines the objectives or purpose of the APP.

Disclosure to third parties

APP 3(5) provides that an entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency—the entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to collect the information other than from the individual; or

(b) it is unreasonable or impracticable to do so.

The LIV considers that APP 3(5)(b) requires clarification about when it is "unreasonable or impracticable" for an entity to collect personal information from an individual so that an entity can instead collect personal information from a third party. The LIV notes that the scope of subcl (b) does not expressly restrict an entity from on-selling to a third party entity personal information obtained from an individual if it is "unreasonable or impractical" for the third party entity to collect the information from an individual. Under the current construction, it may be possible for entities that do not have time to collect information to purchase the same information from another entity

because direct collection is “impractical”. The LIV is concerned that individuals will not have control over where information about them goes and how it is used.

The LIV recommends that guidance be provided on the circumstances in which collection from an individual is deemed to be “unreasonable or impracticable” under APP 3(5)(b).

APP 5 - notification of the collection of personal information

At present, APP 5(1) states at or before the time or, if that is not practicable, as soon as practicable after, an entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subsection (2) as is reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters”.

The LIV recommends that “collects” be changed to “receives” to ensure consistency with earlier provisions and also ensure that APP 5 applies to both solicited and unsolicited information.

We note that APP 5 requires notification only of the matters listed in APP 5(2). APP 5(2)(e) requires an entity to advise the individual of the main consequences of not providing certain personal information. An individual therefore has the option whether to proceed to deal with an entity, where the notification occurs at the time the entity collects personal information about the individual. There does not appear to be regulation of whether “consequences of not providing certain personal information” are fair and reasonable. As noted in respect of APP 3, an entity may be able to deny full services to an individual if that individual declines to provide personal information, even where that personal information is not necessary to provide the service sought. We recognise that APP 2 and the option of anonymity when dealing with an entity may alleviate this concern. Above, we recommend that APP 5 (2) be amended so that at the time of collection of information, entities are required to notify the individual about their right not to provide identity information.

APP 6 – use or disclosure of personal information

APP 6 provides that if an entity holds personal information about an individual that was collected for a particular purpose (defined as the primary purpose), the entity must not use or disclose the information for another purpose (defined as the secondary purpose) unless certain conditions are fulfilled.

The LIV suggests that the terms primary and secondary purpose require guidance notes to assist entities with compliance in this area. In our experience, there is lack of helpful guidance in this area under similar provisions of the National Privacy Principles. Appropriate use and disclosure of personal information is central to protecting individual privacy and we suggest that broad education initiatives would be useful in this area.

APP 7 - direct marketing

APP 7(1) provides that if an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing unless a number of conditions are fulfilled. It is LIV’s view that APP 7(1) is confusing because of cross-referencing and requires redrafting to improve clarity.

APP 7(2) applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing, including in subclause (c), if the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation. The LIV recommends that amendment is

necessary to clarify that "simple means", in relation to electronic communications, is subject to additional obligations under the *Spam Act* 2003 (Cth).

APP 8 - cross-border disclosure of personal information

The LIV is concerned with the interaction between APP 8, which deals with cross-border disclosures, and cl 19, which purports to give extra-territorial effect to the APPs.

APP 8(1) provides that before an entity discloses personal information about an individual to an overseas recipient, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APP. APP 8(2)(a)(i) states that an entity is not bound to take reasonable steps to ensure that an overseas recipient of personal information collected in Australia does not breach the APPs if the entity reasonably believes that the overseas recipient is subject to a law or binding scheme that protects privacy in a "substantially similar way". Clause 19, however, intends to extend the application of the *Privacy Act* 1988 (Cth) to an act done, or practice engaged in, outside Australia by an organisation that has an "Australian link". The LIV queries which provision prevails in circumstances where an overseas entity is captured by both APP 8 and cl 19.

APP 8(2)(a) further provides that an entity is not bound to take reasonable steps to ensure that an overseas recipient of personal information collected in Australia does not breach the APPs if the entity reasonably believes that there are mechanisms that the affected individual can access to take action to enforce that protection of the law or binding scheme. The LIV queries how, in reality, individuals will be able to access such enforcement mechanisms. While a "binding scheme" may exist in theory, if it is time-consuming, expensive or not applied in a practical sense in the country of receipt, then it does not provide any meaningful protection to individuals. Even if a mechanism such as a Privacy Commissioner exists in the receiving country, it is unrealistic to expect Australians to avail themselves of these mechanisms.

APP 8(2)(d) provides that APP 8(1) does not apply if the entity is an agency and the disclosure of the information is required or authorised by or under an international agreement relating to information sharing and Australia is a party to the international agreement. "Agency" is defined in clause 16 and includes Ministers and Departments of the Commonwealth. The LIV is concerned that the government will be able to avoid compliance with the APPs by entering into international agreements. We note that there is no regulation or requirement that international agreements about information sharing comply with the APP by providing, for example, that information is shared only where it is necessary. The ease with which governments can circumvent the APPs through international agreements is demonstrated, for example, by the Department of Immigration and Citizenship's agreement with five countries to exchange biometric information.[1]

APP 10 - quality of personal information

APP 10(1) provides that an entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the entity *collects* is accurate, up-to-date and complete. APP 10(2) provides that an entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the entity *uses or discloses* is accurate, up-to-date, complete *and* relevant.

The LIV recommends that entities should be obliged to collect, use and disclose only accurate, up-to-date, complete and relevant personal information under APP 10. In the interest of succinctness, subclauses (1) and (2) could be merged to read "an entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information the entity collects, uses or discloses is accurate, up-to-date, complete and relevant".

[1] Senator Chris Evans - Minister for Immigration and Citizenship , *Biometrics testing introduced for protection visa applicants* (5 December 2009) <http://www.minister.immi.gov.au/media/media-releases/2009/ce09104.htm> at 9 August 2010.

APP 12 – access to personal information

APP 12(1) states that if an entity holds personal information about an individual, and the individual requests the information, the entity must provide the individual access to the information. Access may be denied, however, if the entity meets one of the exceptions contained in subclauses (2) and (3).

APP 12(3)(b) provides an exception where giving access would have an unreasonable impact on the privacy of other individuals. The LIV considers that APP 12(3)(b) may be difficult to apply where the information is an opinion about an individual because an opinion is arguably personal information of both the person who holds the opinion and the person who is the subject of the opinion.

APP 12(3)(e) provides an exception where giving access would reveal the intentions of the entity in relation to negotiations with the individual in such a way as to prejudice those negotiations. The LIV is concerned about the broad nature of this provision as there does not appear to be any limitations or parameters about what phase of negotiations the parties are in. For example, do the negotiations need to be on foot, or at least reasonably anticipated before this clause becomes operative?

APP 12(8) allows an entity to charge an individual for access their personal information held by that entity, so long as charges are not excessive and do not apply to the making of the request for access to personal information about the individual. However, an entity is not necessarily precluded from charging unreasonable amounts or profiteering. The LIV suggests that "excessive" be replaced with "reasonably necessary to recoup costs incurred by the entity".

We note that APP 12 is also silent on the issue of safeguards to prevent third parties from accessing personal information held by entities and whether any penalties are imposed on entities that negligently release personal information to a third party who purports to be the individual.

APP 13 – correction of personal information

APP 13 provides that entities must take such steps (if any) as are reasonable in the circumstances to ensure that, having regard to the purpose for which it is held, the information is accurate, up-to-date, complete and relevant, including where the individual requests the entity to correct the information.

APP 13(3)(b) provides that if an entity corrects personal information about an individual that the entity previously disclosed to another entity and the individual requests the entity to notify the other entity of the correction, the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so. APP 13(3)(b) therefore requires the individual to request that the entity notify third parties of a correction. The LIV questions why an individual should have to request this notification, particularly where the individual is unaware of the error or to whom the entity has disclosed information or even that information has been disclosed. Entities should be expected to have better records of disclosures to other entities than individuals. The LIV therefore submits that the obligation should be on entities to notify everyone to whom it has disclosed information of the correction.

The LIV also suggests that there be additional guidance as to the grounds on which an entity can refuse to correct information.

Part B – other relevant provisions

Clause 17

Clause 17 defines "organisation" to exclude a small business operator. We note that the Companion Guide to the Draft states that the exemption for small business will remain and will be considered by the government in its second stage response to the ALRC report.

It is LIV's view that small business operators should not be exempt from privacy compliance obligations. We believe that the nature of information collected, and not the size of the organisation that collects the information, should determine whether restrictions should be imposed on the collection of information. The LIV believes that the small business exemption does not serve any rational policy as it would not diminish any regulatory burden on small businesses and also notes recent amendments in the *Equal Opportunity Act* 2010 (Vic) have removed exemption for small business under discrimination law in Victoria. To ensure all entities that collect personal information are subject to privacy compliance, the LIV recommends that the Draft should be amended to ensure that APP apply to small businesses.

Clause 19

The National Privacy Principles currently apply to an organisation if the act or practice relates to personal information about an Australian citizen or permanent resident. Under the APPs cl 19, the APP will apply if the agency or an organisation has an Australian link. The LIV is concerned that cl 19 might remove some protection for Australian citizens and permanent residents, for example where an Australian citizen or permanent resident provides personal information to an agency that does not have an Australian link.