SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **31**

SUBMITTER

Law Council of Australia

Law Council
OF AUSTRALIA

Via email: fpa.sen@aph.gov.au

The Committee Secretary
Senate Finance and Public Administration Committee
PO Box 6100
Parliament House
Canberra ACT 2600
Australia

Dear Committee Secretary,

I refer to the Committee's invitation to provide a submission in connection with the new Australian Privacy Principles Exposure Draft referred to the Committee by the Senate on 24 June 2010.

I have pleasure in enclosing a submission which has been prepared by the Privacy Law Committee of the Business Law Section of the Law Council of Australia ('the Committee'). Please note that the submission has been endorsed by the Business Law Section. Owing to time constraints, the submission has not been reviewed by the Directors of the Law Council of Australia Limited.

If you have any questions in relation to the submission, in the first instance please contact the Committee Chair, Duncan Giles, on 02-9225 5392.

Yours faithfully,

Bill Grant
Secretary-General

17 August 2010

Enc.

GPO Box 1989, Canberra
ACT 2601, DX 5719 Canberra
19 Torrens St Braddon ACT 2612

Telephone +61 2 6246 3788
Facsimile +61 2 6248 0639

Law Council of Australia Limited
ABN 85 005 260 622
www.lawcouncil.asn.au

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

---

Law Council of Australia
Business Law Section
Privacy Committee

17 August 2010

Table of Contents

Introduction

This is a summary of the Committee's suggestions in relation to the Exposure Draft of the Australian Privacy Principles (**APPs**) to be included in *the Privacy Act 1988* (Cth) (**Act**).

The Committee welcomes the reforms that respond to calls that the law should be more consistent and less complex. Many of the comments set out below are guided by that objective.

For ease of reference, we have set the comments by reference to each APP, even where the particular APP has not generated a specific comment.

General Comments

State and Territory law

The Committee is disappointed with the statement in the APPs Companion Guide under the heading "Interaction with State and Territory Laws" on page 19 that:

> *"section 3 of the existing Privacy Act preserves the effect of any State or Territory law that makes provision about interferences with privacy, if it is capable of operating concurrently with the existing Privacy Act. The Government does not intended to change its policy in this regard, so an equivalent provision to this effect will be included in the new Privacy Act."*

The Committee is concerned to ensure that the present reforms result in a single national scheme for privacy regulation. The inclusion of a provision equivalent to Section 3 of in the new Act has the ability to undermine such an outcome.

Complexity, numbering and consistency

As stated on page 1 of the APPs Companion Guide, one of the aims of the reforms is to respond to calls that the law should be more consistent and less complex. The Committee is concerned with the length and complexity of the APPs. This detracts from the intention to draft the APPs as principles based legislation in plain English. The intention is particularly important in the current context as the purpose of the legislation is to give meaning to the privacy rights of individuals. The Committee is of the view that the length and complexity will discourage those outside the legal profession from reading and engaging with the APPs. The length and complexity is also likely to make it harder for organisations and agencies to comply with the APPs. The Committee appreciates that the Privacy Commissioner intends to establish user-friendly guidelines; however it is also important that the legislation itself is clear and not unwieldy. This helps reduce the need for additional guidance and assists with compliance.

The Committee suggests that in the final legislation, the section numbers of each APP correspond to the number of that APP. For example, APP1 should be section 1, or clause 1 (or similar).

The Committee notes that the APPs sometimes require an entity or organisation to "take such steps as are reasonable" and at other times require an entity to "take such steps (if any) as are reasonable".

The Committee is concerned that, in these circumstances, the latter phrase implies that no steps could be reasonable, while the former phrase does not carry such an implication.

The Committee suggests that an entity or organisation only be required to "take such steps (if any) as are reasonable" in all cases. For this reason, the words "(if any)" should appear after the words "take such steps" throughout the APPs.

APP1

The Committee is concerned with the strength and mandatory nature of the language used in section 2(2)(a).

Section 2(2)(a) provides that an entity must take 'such steps as are reasonable in the circumstances to implement practices, procedures and systems...that will ensure that the entity complies with the Australian Privacy Principles". The Committee suggests that it is not possible for practices, procedures and systems to ensure compliance with the APPs. The Committee suggests that words "will ensure" be replaced with the words such as "have the primary purpose of promoting compliance".

The Committee is concerned with the prescriptive nature of the matters to be contained in an entity's privacy policy. Section 4 states that the "privacy policy must contain the following information....".

The Committee suggests that the privacy policy should only be required to contain "reasonable information" or "general information" about the various matters listed.

APP2

No comment.

APP4 to 6

The Committee is concerned that the requirements in APPs 4 to 6 relating to collection do not, expressly permit the sale of a medical business as a going concern.

The Committee suggests that the Act (whether as part of the APPs or elsewhere) specifically allow the collection of sensitive information in circumstances where an entity is buying a medical business as a going concern. Principle 10 in the *Health Records Act 2001* (Vic) and Principle 11 of the *Health Records (Privacy and Access) Act 1997* (ACT) provide useful examples of how this issue might be addressed.

APP6

The Committee supports the inclusion of section 7(2)(d) allowing an entity to use or disclose personal information about an individual if the entity suspects unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities is or may be engaged in, and the entity reasonably believes that the use or disclosure of the information is necessary for the entity to take appropriate action in relation to the matter.

The omission of a section of similar breadth in NPP2 has caused significant issues for organisations.

The Committee is concerned that sections 7(2)(h) and 7(2)(i) are not broad enough to capture all disputes before alternative dispute resolution bodies, tribunals or external dispute resolution schemes.

To promote the use of all alternative dispute resolution options, the Committee suggests that an organisation should be allowed to use or disclose personal information if (in the entity's opinion) it is reasonably necessary for the purposes of a dispute before these bodies.

APP7

No comment.

APP8

The Committee is concerned about the operation of section 9(1), when read in conjunction with section 20 (currently headed 'Acts and practices of overseas recipients of personal information' in the draft). The concern is that compliance with the requirements of section 20 as drafted could make sales of Australian business assets (that include any amount of personal information) practicably unworkable in some circumstances. The onus placed is stricter that that under the APEC framework

The committee suggests that section 20 is unnecessary if the provisions of section 9 have been complied with or, alternatively, that section 20 be redrafted to ensure that sales of business assets not be unnecessarily encumbered.

Reasonable Steps

Under APP8 there is an obligation upon an entity to 'take such steps as are reasonable in the circumstances to ensure that the overseas recipient (of personal information) does not breach the APPs.

An entity is not required to take those steps in a limited number of circumstances which include obtaining consent or where the overseas recipient is subject to a law or binding scheme that has the same effect as the APPs and which can be enforced. There are two exception under the current National Privacy Principle, which are not included in the new APP.

These are:

(a) transfer is necessary for the performance of a contract between the individual and the organisation, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(b) the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the individual between the organisation and a third party.

The net effect of the new provision is that if an entity needs to disclose personal information which is necessary for the conclusion of the contract with an overseas entity which is not subject to a scheme which is similar to the APPs the entity will need to obtain consent or to enter into a contract which will ensure the overseas recipient does not breach the APPs.

There are a number of circumstances where this would be impracticable. The most obvious one is where the organisation is engaged in the travel industry. Such organisations are constantly dealing with overseas entities which are not subject to laws which are similar to the APPs and where it would be impracticable to obtain a contractual obligation from those entities in relation to the observance of the APPs. There would be numerous occasions, also, where it was not possible to obtain consent from the individual such as where arrangements have to be changed at short notice for a variety of reasons, or where an individual would be astonished if

he or she was asked for a related consent in circumstances where they wanted bookings made on their behalf.

We submit that the exceptions referred to above should be included with the new APPs.

APP9

The Committee supports the inclusion of section 10(2)(a) expressly permitting an organisation to use or disclose a government related identifier of an individual where reasonably necessary to verify the identity of an individual for the purposes of the organisation's activities or functions.

This section is important because it allows organisations to more easily comply with their obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)*. In particular, this section will more easily allow organisations to use online customer verification tools for AML compliance purposes.

APP10

No comment.

APP11

No comment.

APP12

No comment.

APP13

The Committee is concerned with the potentially heavy burden imposed by section 14(3).

Section 14(3) requires an entity that has corrected information about an individual to take, on request, steps to notify the correction to any other entity to which it has disclosed that information (unless impracticable or unlawful).

The effect of this requirement may also be to discourage some entities from keeping records about the disclosure of personal information to third parties so as to make it impracticable to notify them about the correction of personal information.

Definition of personal information

This is a central definition in that it determines the scope of the whole Act. The new definition should **only** be accepted by the Senate Committee on the basis that the Committee supports the position that the new definition is **not** intended to change the scope of the existing concept (as set out in section 6 in the Privacy Act). This should be supported by an express and official statement that would be available to assist in interpretation (under the Acts Interpretation Act) to the effect that the change in drafting was not intended to change the meaning.

The Committee notes that the Companion Guide seeks to elaborate on the definition as follows: "The 'reasonable' test limits possible identification based on the context and circumstances. While it may be technically possible for an entity to identify a person by the information it holds, it may be that it is not practically possible (for example due to logistics, legislation or contractual restrictions). The test requires consideration of all the means that are reasonably open for an information holder to identify an individual.

The emphasis is important in that it builds an element of instability into the core definition in the Privacy Act. If the intention is to substantially expand the scope of what is personal information and hence covered by the Act, it would be highly desirable for that to be expressly clear. If so, this needs to be repeated in the Act itself, or at least in the explanatory material that may be used to guide the interpretation of the Act. It should be open to an entity to have arrangements in place to have separate collection and use of multiple non-identifying pieces of information about an individual and that in those circumstances, the information in question should not be considered a collection and use of 'personal information' to which the Privacy Act applies. For example, this would be relevant where the provider contractually undertakes to the user not to collate such information and associate that collation with an individual (even if it was technically feasible for the provider to link that collation to an individual if the provider aggregated and associated such pieces with an individual). The Committee recommends that the test of reasonableness should be the subject of qualification, namely that contractual restriction preventing such collation should be recognised and given practical effect, by expressly factoring in relevant contractual obligations.

The Committee would welcome further consultation prior to the promulgation of any relevant Guidelines relating to the definition of personal information.

Extra-territorial operation of the Act

The Committee is concerned about the extended coverage of the Act in section 19.

The effect of section 19 is that the Act extends to any act done, or practice engaged in, anywhere in the world by an organisation that falls within section 19(3)(g) (i.e. the organisation carries on business in Australia and collects or holds personal information in Australia). This is so whether or not that act or practice or the organisation relates to personal information that was collected or held in Australia by the organisation, or personal information about an Australian citizen or a permanent resident.

The Committee suggests that the Act should only extend to acts done or practices engaged in by organisations that fall within section 19(3)(g) if the act or practice relates to the personal information that was collected or held in Australia by the organisation, or personal information about an Australian citizen or a permanent resident.

Geographical nexus to Australia

The Bill as currently drafted, would relevantly change the geographical nexus provisions of Australian privacy law. Under the Privacy Act 1988, an act or practice of an organisation that takes place outside Australia is not an interference with the privacy of an individual if the act or practice is required by the applicable law of a foreign country (sections 6A(4) and 13D), but there is no clear territorial nexus for "an organisation" (section 6C) and the exception only applies to acts or practices required by foreign law (i.e. response to subpoena or other legal compulsion), not acts permitted in that jurisdiction. The proposed new legislation proposes to pick up the policy in relation to acts and practices required by foreign law and replicate that policy as provisions in the new Privacy Act. The relevant provisions to give effect this policy do not appear in the Exposure Draft but their intended operation is summarised on page 7 of the Companion. However, the proposed new Act would also include the concept of "Australian link" in a new extra-territoriality provision, clause 19(1), which would apply the Australian Privacy

Principles to "an organisation that has an Australian link", being (relevantly) a body corporate incorporated in Australia (cl.19(3)(e)), and an organisation that both "carries on business in Australia" and "collects or holds personal information in Australia whether before or at the time the act is done or the practice is engaged in" (clause 19(3)(g)). In both of these cases, the personal information may not in fact relate to an Australian individual, as the "Australian link" relates to the organisation, not the particular individual that is the data subject. It seems undesirable that an Australian corporation be regulated in respect of its overseas data collection activities merely on the basis that it is an Australian corporation, even where activities are legal in the place in which those activities occur, the data does not touch Australia and does not relate to the personal information of an individual in Australia.

Disclosure of personal information required by foreign law

Disclosure under compulsion of Australian law is permitted, but not disclosure under compulsion of foreign law. This compounds the problem noted above, as (for example) a US office of an Australian corporation responding to US court process could find itself in jeopardy under Australian law (again, even if the data subject was not an Australian person or a person living in Australia). The Committee recommends that disclosures required under any law or legal process applicable to the organisation should be expressly permitted.

Location of the collection of personal information

The second limb of clause 19(3)(g)) is very difficult to interpret and apply in relation to international internet services. When a collector "collects" personal information about an Australian user, it is unclear if the act of collection is taking place in Australia or at the place at which the information is collated and processed. Although there is a strong argument that the act of collection takes place at the place at which the information is collated and processed, it could be argued that the act of collection takes place at the point at which the information is collected, applying (with a stretch!) analogous reasoning to the multiple publication "rule" accepted by the High Court of Australia in the Gutnick case in respect of defamation under Australian law. The Committee submits that it would be preferable if the Act made it clear that the act of collection occurs at (say) the place at which the information is collated and processed, and not the location of the individual (that is, not the location from which the information is collected). The point of collection is often fortuitous and often cannot be ascertained - as an IP address or other geographically locating information in respect of a particular internet transaction may not be sufficient to enable the internet service provider to identify the location of the user and thereby ensure that it complies with local law applicable in that location.

Acts and practices of overseas recipients of personal information

Clause 20(2)

Clause 20(2) deems any act or practice in relation to the information that would be a breach of or non-compliance with the APPs (if they applied to that overseas recipient) by the overseas recipient to be an act done or a practice engaged in by the disclosing entity. However, where the disclosing organisation takes such steps as are reasonable in the circumstances, that disclosing organisation may nonetheless be liable in relation to any breach of or non-compliance with the APP by the recipient. This is an inequitable outcome but appears to flow naturally from the drafting. The Committee recommends that the clause be specifically redrafted to provide protection to the disclosing part where that party has taken reasonable steps to respect privacy compliance.

The Committee is concerned that an entity may be liable for an act done or practice engaged in by an overseas recipient of personal information, even where the entity has complied with section 9(1) (APP8) by taking such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs in relation to the information.

The Committee suggests that in circumstances where the disclosure by the entity of information to an overseas recipient complies with section 9(1), the entity should not be liable for any acts done, or practices engaged in, by the overseas recipient in relation to that information.

Similarly, the Committee is concerned that should the entity be liable, there is no time period after which an entity will no longer be liable for the acts done or practices engaged in by an overseas recipient of personal information. This has particular implications for sale of businesses to overseas purchasers. The Committee suggests that the liability imposed by section 20 should be limited in time and aligned to the statutory limitation periods as they currently exist (either under the Trade Practices Act, being 3 years or under the various privacy regimes giving an individual 6 or 12 months to bring a complaint).