Inquiry into the Australian Privacy Principles Exposure Draft

Submission to the Senate Finance and Public Administration Committee

by

Law Council of Australia

Business Law Section

Privacy Committee

25 March 2011

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

Introduction

The Committee is grateful for the opportunity afforded by the Senate Finance and Public Administration Committee to expand upon the comments that have previously been provided.

Following submissions dated 17 August 2010 (**First Submission**), the Law Council of Australia Privacy Committee (the **Committee**) has further discussed the Exposure Draft of the Australian Privacy Principles (**APPs**) and considers it may be of assistance if we set out our concerns in slightly more detail.

The Committee also wishes to note that any comments cannot be considered final until the proposed legislation is presented in its entirety and considered as a whole. The effect of and interpretation of the APPs is difficult to consider in the absence of the administrative regime that surrounds them, and without the full suite of "specific industry" provisions that it appears may add to, subtract from, or replace them altogether.

General Further Comments

Structure and Drafting of the APPs

As set out in the First Submission, the Committee notes that the simple language and structure contained in the current National Privacy Principles (**NPPs**) has been abandoned in favour of a more verbose and complex set of principles.

The Committee submits that the structure and drafting of the APPs should be reviewed with the aim of reverting to the simpler drafting style in the NPPs. That structure and language is based on and referable to the original OECD guidelines on which many State and Territory and International equivalents are based. Many of the distinctions in the proposed legislation appear unnecessary, making the proposed new principles difficult to interpret, and therefore less accessible to ordinary members of the public at large, to privacy practitioners, regulated organisations and consumers.

For instance, APP 2 sets out the following:

> '*Australian Privacy Principle 2 – anonymity and pseudonymity*
>
> *(1) Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an entity.*
>
> *(2) Subsection (1) does not apply if:*
>
> *(a) an entity is required or authorised by or under an Australian law, or an order of a court or tribunal, to deal with individuals who have identified themselves; or*
>
> *(b) it is impracticable for an entity to deal with individuals who have not identified themselves.*'

This replaces NPP 8, which provides:

> '*Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.*'

It seems unnecessary to replace NPP 8 with the more verbose APP 2 while the meaning remains essentially unchanged.

APPs 3 and 4 now distinguish between the collection of '*solicited*' personal information and '*unsolicited*' personal information. This has resulted in a far wordier principle than

NPP 1. We submit that the distinction between the collection of solicited and unsolicited personal information should be removed by deleting APP 3(6) and APP 4.

A further instance of unnecessary verbiage appears at APP 3(1), which provides:

> *'Australian Privacy Principle 3—collection of solicited personal information*
>
> *Personal information other than sensitive information*
>
> *(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.*'

This provision equally applies to sensitive information and APP 3(2)(a)(i) merely repeats those provisions contained in APP 3(1), as below:

> *'(2) An entity must not collect sensitive information about an individual unless:*
>
> *(a) both of the following apply:*
>
> *(i) the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities;*
>
> *(ii) the individual consents to the collection of the information; or*
>
> *(b) subsection (3) applies in relation to the information.'*

Yet another instance of excess verbiage is contained at APP 3(5), set out below:

> *'(5) 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.*'

This provision is far more wordy and convoluted than the original NPP 1.4, which provides:

> *'1.4 If it is reasonable and practicable to do so, an organisation must collect personal information about an individual only from that individual.'*

The drafting of APP 7 (in relation to direct marketing) also may cause confusion. It seems nonsensical to have separate principles relating to personal information collected for the purposes of direct marketing and personal information collected for other purposes. We submit that APP 7 be deleted and instead appropriate direct marketing requirements be included in APP 6 in the same way they are included in the current NPP 2.1. (This Committee has long supported appropriate measures to apply direct marketing restrictions consistently, regardless of the purpose of collection. Our comment is directed merely to the implementation of that policy change, which we submit could be achieved in a manner that would be understood by a non-expert within the generally applicable APP).

As set out in the First Submission, the numbering of the APPs should correspond with the section numbering in the legislation to avoid confusion about the applicable APP. The Committee believes that this is not a concern about form over substance but a real issue that is important to the comprehensibility of the APPs by ordinary readers. Useability by the intended audience must be an important consideration in the production of all documents, and we submit it is most important in the case of contractual documents and legislative documents where sanctions apply for non-compliance.

Cross-Border disclosure of Personal Information

The proposed APPs place onerous requirements on Australian entities disclosing information to overseas entities to ensure the overseas entity does not breach the APPs. In order to achieve this, the Australian entity would have to require the overseas entity to bind itself to observe the APPs. We believe that this would be an onerous requirement for an affected foreign entity which many may resist. Accordingly, we submit APP 8(1) should be redrafted to require less onerous but still effective requirements as follows:

> *'(1) Before an entity discloses personal information about an individual to a person (the overseas recipient):*
>
> *(a) who is not in Australia; and*
>
> *(b) who is not the entity or the individual;*
>
> *the entity must take reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information in a manner which is inconsistent with the Australian Privacy Principles.'*

The exemptions which are the current NPP 9.1(c) and (d) have not been included in the APPs, for no apparent reason. APP 8(2) should be amended to include the following:

(a) *'the 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*'; and

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

We also take the opportunity of restating our submission that Clause 20 of the draft Bill should be redrafted to provide that, where an entity has taken reasonable steps to respect privacy compliance that entity should not be liable for any acts done, or practices engaged in, by the overseas recipient in relation to that information.

As a related matter, we note that the credit reporting provisions (in some cases) supplant the APPs and (in other cases) are expressed to apply simultaneously with them. It may be (although the Committee would prefer that this approach be avoided) that additional specific parts of the privacy legislation - such as the forthcoming health provisions - will also be drafted so as to fragment the legislative requirements.

The Committee submits that if different provisions are to apply in addition to, or instead of, the APPs, that the provisions dealing with offshore use or disclosure should not apply a different standard than what the transferor organisation is subject to in Australia in relation to the relevant information.

Conclusion

For reasons outlined above the Committee submits that it would be desirable to draft the new APPs as principles based provisions closely following the OECD structure. This will assist with meeting the objectives of clarity and simplification. The Committee submits that clear and simple provisions assist the business and legal community to comply with legislation, thus giving practical meaning to legal rights and therefore enhancing privacy protections afforded to individuals.