SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **29**

SUBMITTER

Privacy NSW

submission

Submission by Privacy NSW to

Senate Finance and Public Administration Legislation Committee

privacynsw

Issue date: 13/8/10

Christine McDonald
Secretary
Senate Finance and Public Administration Legalisation Committee
PO Box 6100
Parliament House
CANBERRA ACT 2600

Enquiries: Siobhan Jenner
Tel: (02) 8019 1903
Our ref: A10/0859
Your ref:

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

Dear Ms McDonald

Re: Submission on the Australian Privacy Amendment Legislation

We are pleased to provide the following submission on the exposure drafts of the Australian privacy amendment legislation.

We welcome the Australian Government's initiatives to harmonise privacy laws in Australia to date. We have previously provided submissions in response to the Australian Law Reform Commissioner's (ALRC) *Discussion Paper 72*[1] and to the Commonwealth Attorney General's Department consultation on the then proposed Unified Privacy Principles (UPPs) and related matters[2].

While the Australian Privacy Principles (APP) Companion Guide does explicitly refer to the recommendation by the ALRC regarding a Commonwealth-State cooperative privacy scheme[3], our views in this submission are made with a view to the potential impact on the privacy landscape in NSW, as mooted by the ALRC:

> Recommendation 3–4: The Australian Government and state and territory governments, should develop and adopt an intergovernmental agreement in relation to the handling of personal information. This agreement should establish an intergovernmental cooperative scheme that provides that the states and territories should enact legislation regulating the handling of personal information in the state and territory public sectors that:
>
> > (a) applies the model Unified Privacy Principles (UPPs), any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act* as in force from time to time…

In interim, we embrace the process of privacy law reform as a prime opportunity to create accessible privacy law, with an emphasis on personal control, rather than institutional convenience and on ease of understanding rather than specialised knowledge.

---

1 http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/ALRC_submission_on_DP72_Dec07.pdf/$file/ALRC_submission_on_DP72_Dec07.pdf. (ALRC submission)

2 Submission to the Department of Prime Minister and Cabinet (DP&C submission), 11 March 2009.

3 *Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, Recommendation 3-4.

privacynsw

This submission firstly provides comment on definitions in Part B of the draft legislation which have a direct correlation to some of our comments on the APPs which follow.

Definitions

Consent

We note that this definition is the same as it appears in the *Privacy Act 1988* (Cth) (the Privacy Act). There is no such definition in the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act). The inclusion of a definition of consent underscores the central role that individuals should play in relation to dealing with their personal information. However, while we support the inclusion of a definition of consent we believe that a mere definition of consent as a choice between 'implied' or 'express', does not enable entities to ascertain whether an individual does in fact understand and or agree to a particular dealing with their personal information. Without further definition, entities may rely on implied consent, construing agreement from possibly irrelevant or non-existent considerations. We therefore suggest that the terms 'implied' and 'express' consent be defined and that there be separate reference to these definitions in the principles to which they apply. For instance, in the case of the collection of sensitive information, it is our view that entities should be required to obtain express consent to a particular dealing with that information, unless the entity can reasonably rely on a relevant exception. In circumstances where an individual lacks the capacity to provide express consent (for instance through disability or age), we suggest that there be an exception which permits collection if the entity has obtained express consent from an authorised representative who is empowered to make substitute decisions on behalf of the individual. We suggest that there be an Australian Privacy Rule[4] which governs the means by which an entity be satisfied it is dealing with an authorised representative.[5]

Entity

We note the advice in the Companion Guide that the policy in section 16E of the *Privacy Act* will reflected in the new Act, thereby excluding individuals acting in the context of 'personal, family or household affairs' from jurisdiction. We suggest that this might be more readily effected by including a similarly worded exclusion in the definition of an 'entity' rather than by a separate provision.

Personal information

The draft definition of personal information includes 'information or an opinion about an identified individual, or an individual who is reasonably identifiable'. We suggest that the last part of the definition should be tied to the information at issue by including the words ' from the information or opinion'. Without these words there is no context for the 'reasonably identifiable' part of the definition.

[4] As referred to in APPs 3 & 6 and defined in Part B.
[5] This is consistent with our ALRC submission (pp 45-48) DPC submission (p 2). On this issue Privacy NSW has issued a Best Practice Guide: *Privacy and People With Decision-Making Disabilities* which provides guidance for NSW public sector agencies about making decisions about capacity to consent.

privacynsw

The definition of 'personal information' in the *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) excludes certain categories of information, such as information about individuals who have been dead for more than 30 years, which means that the Information Protection Principles which follow are not encumbered by repeated references to those exclusions. In drafting terms there is a clear demarcation between the 'exemption' which ties to categories of excluded information or bodies, and the 'exceptions' which tie to particular circumstances in which an IPPs will not apply.

Australian Privacy Principles (APPs)

APP1 - open and transparent management of personal information

We support the placement of an openness principle at the start as it establishes up front the importance of planning prior to the point of dealing with personal information.

We also support the inclusion of a provision requiring entities to advise individuals about the means of bringing a complaint about an interference with their privacy as this is likely to enhance openness and accountability on the part of entities.

We further support the inclusion of a requirement to advise whether personal information may be disclosed outside Australia and if so, where the recipients are located. However we suggest (as noted below regarding APP 8) that personal information should only be disclosed outside the jurisdiction in which the subject individual resides if the receiving jurisdiction has privacy legislation which affords the same level of protection as the APPs.

APP 2 – anonymity and pseudonymity

We support this principle.

APP 3 – collection of solicited personal information

(1) - (3): In our view, the complex wording of this APP defeats the purpose in choosing principle-based rules rather than legislation. As noted above, in our view privacy principles should be drafted with a view to them being read and understood by the general public rather than by lawyers. We therefore suggest that this principle could be more simply expressed, firstly by stating what may be collected (ie that which is 'directly related to functions or activities', omitting the word 'reasonably') followed by a brief reference to conditions attaching to the collection of sensitive information starting with consent, for example:

Sensitive information may only be collected with the express consent [see comments above] of the individual, or if the following exceptions apply [including a reference to the authorised representative test in the Australian Privacy Rules as suggested above].

(4): We support this sub-principle.

(5): We support this sub-principle.

(6) We suggest that this sub-principle could be removed if there were a simple amendment excluding un-solicited information from the definition of personal information.

APP 4 – receiving unsolicited personal information

In our experience it is sometimes appropriate for agencies to return unsolicited personal information to the sender rather destroying it. In some cases the sender will be the person to whom the information relates, but in other cases it will be third party information. In our view the key to resolving the issue is to involve the individual as far as possible in decisions regarding their information.

APP 5 – notification of the collection of personal information

(1)– (2) We support this principle but suggest that it be simplified, ie:

> When an entity collects personal information it must notify the individual about the following matters, unless it is reasonably unable to do so [suggest that there be a reference to guidance by the Privacy Commissioner on these matters]: …

We also suggest that this is the best opportunity for an individual to exercise express consent to intended uses and disclosures. We suggest that this could take the form of an 'opt-in' box for intended primary uses and or disclosures, or possible secondary uses and/or disclosures.

APP 6 – use or disclosure of personal information

Again, we believe this principle is too complex to be of benefit to the general public in understanding what might happen to their personal information. In order to remedy this we suggest that the principle should start with a link to APP 5, ie:

> If an entity has notified an individual about its intended uses or disclosure of personal information it may carry out those uses or disclosures. If an individual has not agreed to those uses or disclosures, the entity may only use or disclose the information if the following circumstances apply: …

We support sub-principle (3) in relation to the recording of the secondary use or disclosure of personal information for the purpose of sub-principle (2)(e), however we suggest that this requirement be extended to any circumstances in which personal information is used or disclosed for a secondary purpose.

APP 7 – direct marketing

In our discussion with DP&C[6] we suggested that direct marketing should be viewed as merely another circumstance in which the prohibition on secondary use or disclosure may be exempted. In our view it should not be a separate principle, as the presence of a separate principle for direct marketing may cause confusion as how APP 6 might also

[6] 5 February 2009.

apply. If direct marketing is included in APP 6, the circumstances in sub-principles (1) – (6) could be contained in an Australian Privacy Rules.

APP 8 – cross border disclosure of personal information

As it is currently APP 6 does not link to the purpose for which it was collected or to matters about which the individual was notified. Rather it starts with the assumption that the information may be disclosed outside Australian as long as the recipient does not breach the APPs. Given the potentially serious impact of a disclosure of personal information outside Australia, we believe that this principle should be more stringent, not less stringent than APP 6.

As noted above, we take the view that personal information should only be disclosed outside the jurisdiction in which the subject individual resides, if the receiving jurisdiction has privacy legislation which affords the same level of protection as the APPs, or if the individual has provided their express consent.

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

We support this principle but suggest that it be simplified, removing the matters sub-principles (2) – (3) to Australian Privacy Rules and sub-principles (4) –(5) be removed to the definition section.

APP10 – quality of personal information, APP 11 – security of personal information

The Companion Guide states that the layout of the principles reflects the information cycle. Requiring entities to ensure the quality and security of information after decisions about use, disclosure, access and correction does not follow this logical sequence. To better reflect the information cycle we suggest that the quality principle and the security principle should be placed after the notification principle and before the use and disclosure principle.

APP 12 – access to personal information, APP 13 – correction of personal information

We support this principle, but again note that the exceptions to the requirement to provide access are dense and complex.

We also note the advice in the Companion Guide that the *Freedom of Information Act (Reform) 2010 (Cth)* will commence on 1 November 2010 and that matters relating to access and correction are currently subject to 'a large number of technical issues'. In New South Wales the *Government Information (Public Access) Act 2009* commenced on 1 July 2010. It provides that there is a public interest consideration against the disclosure of government information which would 'contravene an information protection principle under the *Privacy and Personal Information Protection Act 1998* or a Health Privacy Principle under the *Health Records and Information Privacy Act 2002*'[7].

[7] Section 14(3), Table clause 3.

Other matters

Data breach notification

While not specifically referred to in the Companion Guide, we take this opportunity to express our view that there should be an APP requiring entities to report data breaches. In our submission to the ALRC we supported the inclusion of provision in the *Privacy Act* to allow for data breach notification, whereby agencies and organisations would be required to report security breaches to affected individuals.[8] Having reviewed the draft APPs and noting the potential for harm to individuals following a data breach, it is our view that this provision ought to be expressed as an APP, as it concerns action that should be taken by an entity in relation to its dealings with the personal information of its clients.

Exemptions

We also take this opportunity to state our continued support for the removal of the employee records exemption and the small business exemption from the Privacy Act[9].

We hope you find our comments on these matters of assistance to you in moving toward a new privacy law for Australia, and we invite you to contact Ms Jenner of this Office on (02) 8688 8576 if you have any queries regarding this submission.

Yours sincerely

John McAteer
Acting Privacy Commissioner

[8] See ALRC submission at pp 41-42.
[9] See ALRC submission at pp 34-35.

privacynsw

privacynsw