office of the privacy commissioner
new south wales

Enquiries: Jessica Falvey
Tel: (02) 8071 7024
Our ref: A12/0655

Ms Julie Dennett
Committee Secretary
Senate Standing Committee on Legal and Constitutional Affairs
PO Box 6100
Parliament House
Canberra ACT 2600

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

Dear Committee Members

Submissions on the Privacy Amendment (Enhancing Privacy Protection) Bill 2012

Thank you for providing us with an opportunity to make submissions on the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (**the Bill**).

We welcome the government's initiatives to harmonise privacy laws in Australia and we appreciate the government's work to date on this important and challenging law reform project.

We are generally pleased with some of the proposed amendments in the Bill that seek to clarify and enhance privacy protection in Australia. However, other aspects of the Bill potentially weaken existing privacy protections afforded to the Australian public or are drafted in a way that could create loopholes or uncertainties.

In 2010, we made submissions to the Senate Standing Committee on Finance and Public Administration on the exposure draft of the Australian Privacy Principles (**APPs**).[1] Unfortunately, a number of the issues that we raised at that time do not appear to have been addressed in the Bill. We have therefore restated some of those issues in these submissions, along with raising additional issues.

We have summarised our recommendations in the section below. Further comments and more detailed explanations for our recommendations can be found in the following sections of our submissions.

Our recommendations

1. The language and structure of the APPs and accompanying provisions should be further simplified, for example, by:

    a. removing unnecessary words or phrases;
    b. using simpler language where possible; and

[1] NSW Office of the Privacy Commissioner, *Submission on the Australian Privacy Amendment Legislation* (2010), available at www.privacy.nsw.gov.au.

c. using notes to draw the reader's attention to other relevant provisions, concepts or issues.

2. The personal, family or household affairs exemption in section 16 of the Bill should be included as an exemption from the definition of "entity" rather than as a completely separate provision.

3. The language of sections 16A (permitted general situations) and 16B (permitted health situations) of the Bill should be further simplified. In addition, we recommend including notes in each place within the APPs where a "permitted general situation" or a "permitted health situation" is referred to in order to direct the reader back to the relevant subsections of section 16A or 16B.

4. In APPs 3.1, 3.2 and 3.3, references to the phrase "reasonably necessary" should be replaced with "necessary" and references to the phrase "directly related to" should be deleted.

5. In APP 3.3, the reference to "consents" should be amended to "expressly consents".

6. APP 3.5 should be amended to also include a requirement that personal information must not be collected in an unreasonably intrusive way.

7. APP 4 should include options for entities to:

    a. return unsolicited personal information to the individual in appropriate circumstances rather than destroying or de-identifying it; and
    b. involve the individual in decisions about what happens to their unsolicited personal information, where this is practicable and appropriate.

8. APP 8.1 should be amended to require an entity to enter into a contractual relationship with an overseas recipient unless that would not be reasonable in the circumstances. If this is the case, the entity could take other reasonable steps to ensure that the overseas recipient does not breach the APPs.

9. APP 8.2(a) should be amended to also require an entity to have regard to any guidance material issued by the Privacy Commissioner in relation to overseas laws or schemes that the Commissioner considers to be as stringent as the *Privacy Act 1988*.

10. APP 8.2(b) should be amended to specify that an entity needs to notify an individual of the practical effect and potential consequences of APP 8.1 not applying to a disclosure of personal information outside Australia.

11. A template could be prepared which sets out the form of notification that an entity must give for the purpose of APP 8.2 so that there is consistency in relation to the language and content used by entities. Any such template could either be included in an accompanying Regulation or prepared with guidance from the Privacy Commissioner.

12. In APP 8.2(b), the references to "consents" should be amended to "expressly consents".

13. APP 11.2 should be amended to require an entity to take reasonable steps to not only destroy or de-identify personal information that is no longer required, but also to return the information to the individual, if that is more appropriate in the circumstances.

14. In APP 12.4, there should be a specified timeframe for an organisation to respond to a request for access to personal information, instead of the current requirement for a response within a "reasonable period".

15. When an organisation gives an individual access to their personal information, there should be a specified fee or other guidance on what could constitute an excessive fee for the purposes of APP 12.8. This could be included in an accompanying Regulation or through guidance by the Privacy Commissioner.

16. In APP 13, there should be a specified timeframe for an organisation to respond to a request for correction of personal information, instead of the current requirement for a response "within a reasonable period".

Drafting and structure of the Bill

We support the Australian Law Reform Commission's recommendation that privacy principles should be "simple, clear and easy to understand and apply".[2] It is important for the Australian public to be able to understand the privacy protections afforded to them when dealing with government agencies, businesses and other organisations. Privacy principles should not just be accessible to those who have specialised privacy, legal or other knowledge, rather, they should be accessible to the community as a whole.

Unfortunately, there is a high degree of complexity within the APPs and the accompanying provisions of the Bill. We acknowledge that it is a very challenging task to bring together two sets of privacy principles, particularly where a number of exemptions also apply.

However, we recommend that the language and structure of the APPs and accompanying provisions be further simplified to allow the community as a whole to better understand the privacy protections afforded to them (**see Recommendation 1**).

Preliminary sections to the APPs

Exemption for personal, family or household affairs

Section 16 of the Bill reflects the policy that is currently in section 16E of the *Privacy Act 1988* to exclude individuals acting in the context of personal, family or household affairs from the jurisdiction of the *Privacy Act 1988*.

We recommend that section 16 of the Bill be included as an exemption from the definition of "entity" rather than as a completely separate provision. Our view is that this will achieve further simplicity and consolidate related exemptions so that members of the public do not have to look at multiple provisions to determine whether or not something is regulated by the *Privacy Act 1988* (**see Recommendation 2**).

Permitted general and health situations

[2] Australian Law Reform Commission, *For your information: Australian privacy law and practice,* Report 108 (2008), recommendation 18-1 (**ALRC Report 108**).

Section 16A of the Bill defines a "permitted general situation" and section 16B of the Bill defines a "permitted health situation". These are exemptions to the APPs.

The provisions are quite detailed and complex, particularly section 16B, which breaks the permitted health situations down into further categories such as collection relating to the provision of a health service, collection for research, etc. The complexity of these provisions may make it difficult for the public to understand the nature and effect of these exemptions (**see Recommendation 3**).

Liability of local entities for actions of overseas recipients

We support section 16C of the Bill, which essentially ensures that where a local entity discloses information to an overseas recipient, the local entity will be liable for any breach of the APPs by the overseas recipient.

We hope that this provision will benefit the community by:

- prompting local entities to carry out appropriate due diligence before disclosing personal information to an overseas recipient; and
- encouraging local entities to enter into contractual arrangements to ensure that an overseas recipient will comply with privacy principles/laws that are no less stringent than the APPs.

Australian Privacy Principles (APPs)

APP 1 – 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.

The openness principle also contains a detailed list of matters to be included in privacy policies. In our opinion, the community expects to have easy access to relevant, useful and targeted privacy policies. Such privacy policies are important because, in our experience, privacy breaches often occur in either of the following circumstances:

- where the organisation does not have any privacy policies or training programs for staff; or
- where the organisation has privacy policies or training programs in place, however, they are deficient in some respect, for example, they may not be targeted to the particular privacy issues that the organisation faces.

We also support the provisions that require privacy policies to inform members of the public about:

- how to make a complaint about a possible breach of the APPs; and
- whether an entity is likely to disclose personal information to overseas recipients.

These provisions are likely to enhance openness and accountability on the part of entities.

APP 2 – anonymity and pseudonymity

We generally support this principle, which allows individuals to deal with entities anonymously or using a pseudonym in certain circumstances. The community expects to

have the option of dealing with entities on an anonymous basis in appropriate circumstances. Such anonymous dealings can also prevent entities from collecting and retaining unnecessary personal information about individuals.

APP 3 – collection of solicited personal information

We generally support this principle, however, we have several concerns about the current wording of this principle.

We note that the Australian Law Reform Commission recommended that personal information must not be collected by entities unless it is "necessary" for their functions and/or activities.[3]

APP 3.1 allows government agencies to collect personal information where it is reasonably necessary for, or directly related to, their functions or activities. However, APP 3.2 allows private organisations to do this only where it is reasonably necessary for their functions or activities.

In the equivalent provision of National Privacy Principle 1 and Information Privacy Principle 1, the term "necessary" is used rather than "reasonably necessary".[4] While there is use of the phrase "directly related to" in Information Privacy Principle 1 in relation to agencies, this phrase is not used in National Privacy Principle 1 in relation to organisations.

We are concerned that the current draft of APP 3 will weaken the existing privacy protections afforded to the Australian public in the Federal *Privacy Act 1988*. We consider that this is a good opportunity to ensure that there is consistency between the obligations on agencies and organisations with respect to the collection of personal information. In our view, the community would generally expect the same level of privacy protection irrespective of whether the entity they are dealing with is an agency or an organisation.

In relation to APP 3.1 and APP 3.2, we therefore recommend that the phrase "reasonably necessary" be replaced with "necessary" and that the phrase "directly related to" be deleted. We recommend that the equivalent amendments are also made to APP 3.3 as members of the public generally expect that their sensitive information will be subject to higher than normal levels of privacy protection (**see Recommendation 4**).

In APP 3.3, there is reference to an individual giving consent to the collection of their sensitive information in certain circumstances. Reliance on implied consent is not appropriate in relation to the collection of sensitive information. The reliance on implied consent could lead to an entity construing agreement from possibly irrelevant or non-existent considerations.

We therefore recommend that the reference to "consents" in APP 3.3 be amended to "expressly consents" (**see Recommendation 5**).

APP 3.5 requires entities to only collect personal information by lawful and fair means. However, the current requirements in the National Privacy Principles and the Information Privacy Principles relating to the way in which personal information is collected appear to be more stringent than APP 3.5.

[3] ALRC Report 108 (2008), recommendation 21-5.
[4] See National Privacy Principle 1.1 and Information Privacy Principle 1 in the Federal *Privacy Act 1988*.

For example, in National Privacy Principle 1.2, an organisation must also ensure that it does not collect personal information in an unreasonably intrusive way. Likewise, Information Privacy Principle 3(d) also requires an agency to take reasonable steps to ensure that when it collects personal information it does not "intrude to an unreasonable extent upon the personal affairs of the individual concerned." These requirements are similar to the requirement imposed upon NSW government agencies to take reasonable steps to ensure that the collection of personal information does not intrude to an unreasonable extent on an individual's personal affairs.[5]

In our experience, the community expects that entities (whether private sector organisations or government agencies) will not unreasonably intrude into their personal affairs when collecting personal information. It also creates confusion for members of the community when NSW government agencies must take reasonable steps to ensure that the collection of personal information does not unreasonably intrude into an individual's personal affairs but Commonwealth government agencies and private organisations do not have to adhere to the same standard.

We therefore recommend that APP 3.5 be amended to also include a requirement that personal information must not be collected in an unreasonably intrusive way (**see Recommendation 6**).

APP 4 – dealing with unsolicited personal information

We generally support this principle. It is important for an entity to determine whether it has "collected" a member of the public's personal information so that it can then deal with that information in compliance with the other APPs.

However, members of the public may sometimes prefer to have their unsolicited personal information returned to them, rather than destroyed or de-identified. The key to resolving the issue is to involve the individual as much as possible in decisions regarding their information (**see Recommendation 7**).

APP 5 – notification of the collection of personal information

We generally support this principle as it contains a detailed and relevant list of matters that an entity must take steps to notify an individual of. Such notification is important as members of the public want to know why their personal information will be collected, how it will be used and who it will be disclosed to (particularly if it is likely to be disclosed across borders).

APP 6 – use or disclosure of personal information

We generally support this principle, which deals with the circumstances in which an entity can use or disclose personal information.

APP 7 – direct marketing

[5] See section 11(b) of the NSW *Privacy and Personal Information Protection Act 1998*.

We generally support the regulation of direct marketing from a privacy perspective given that this is a common issue of concern for members of the public.

We have previously submitted that direct marketing should be dealt with as part of the principle relating to use and disclosure of personal information.[6] However, given the detailed wording of the direct marketing principle in the Bill, we concede that it may not be practicable to incorporate the intent of that provision into APP 6.

APP 8 – cross-border disclosure of personal information

We broadly support a privacy principle dealing with cross-border disclosures of personal information, particularly in the current environment where:

- entities are increasingly seeking to outsource some of their functions to jurisdictions outside Australia to take advantage of cost savings; and
- technological advances, such as cloud computing, mean that personal information is increasingly being transferred, or stored, in jurisdictions outside Australia.

The public expects particularly strong controls around disclosures of personal information outside Australia. We consider that the current drafting of APP 8 could be improved to meet these expectations.

APP 8.1 requires a local entity to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. On page 83 of the Explanatory Memorandum it states that the concept of taking such steps as are reasonable in the circumstances will normally require a local entity to enter into a contractual relationship with the overseas recipient. Given that this is usually the safest approach, we recommend that APP 8.1 be amended to require an entity to enter into a contractual relationship with an overseas recipient unless that would not be reasonable in the circumstances. If that is the case, the entity could then take such other reasonable steps to ensure that the overseas recipient does not breach the APPs (**see Recommendation 8**).

APP 8.2(a) provides an exemption to APP 8.1 where the local entity reasonably believes that the overseas recipient is subject to a privacy law or binding scheme that is substantially similar to the way in which the APPs protect the information. If personal information is disclosed to an overseas recipient, the community would generally expect that the privacy law or scheme in the receiving jurisdiction would be no less stringent than the *Privacy Act 1988*. We recommend that APP 8.2(a) be amended to also require an entity to have regard to any guidance material issued by the Privacy Commissioner in relation to overseas laws or schemes that the Commissioner considers to be as stringent as the *Privacy Act 1988* (**see Recommendation 9**).

We are also concerned about APP 8.2(b), which allows an individual to consent to the disclosure of their personal information to an overseas recipient if the local entity has expressly informed the individual that the protections in APP 8.1 will not apply to the disclosure. We are concerned that entities might include this notification requirement in general privacy policies or other legal documents. Individuals may then "agree" to something which may be buried in the middle of a privacy policy or legal document and may be drafted in complicated language, rather than plain English.

[6] See for example, NSW Office of the Privacy Commissioner, *Submission on the Australian Privacy Amendment Legislation* (2010) available at www.privacy.nsw.gov.au.

In addition, we do not think that it is sufficient for an entity to merely inform the individual that APP 8.1 will not apply to a cross-border disclosure of personal information. We suggest that an individual needs to be given a plain English explanation of:

- the practical effect of APP 8.1 not applying to the disclosure; and
- the potential consequences of APP 8.1 not applying to the disclosure.

We therefore recommend that APP 8.2(b) be amended to specify that an entity needs to notify an individual of the practical effect and potential consequences of APP 8.1 not applying to a disclosure of personal information outside Australia (**see Recommendation 10**).

We also recommend that a template be prepared which sets out the form of notification that a local entity must give for the purpose of APP 8.2 so that there is consistency in relation to the language and content used by entities. We recommend that this template could be included in an accompanying Regulation or prepared with guidance from the Privacy Commissioner (**see Recommendation 11**).

We also consider that implied consent would not be appropriate in the circumstances of APP 8.2(b) as the community expects a higher level of privacy protection in relation to the movement of their personal information outside Australia. Reliance on implied consent could lead to an entity construing agreement from possibly irrelevant or non-existent considerations. We therefore recommend that the references to “consents” in APP 8.2(b) be amended to “expressly consents” (**see Recommendation 12**).

The above recommendations will assist in ensuring that members of the public are:

- adequately notified in relation to the practical effect and potential consequences of consenting to APP 8.1 not applying to a cross-border disclosure of their personal information; and
- able to give their informed consent to such an act.

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

We generally support this principle, which restricts the adoption, use and disclosure of government related identifiers by private sector organisations. Without this principle, there would be a risk to the community of government related identifiers becoming a widespread method of identifying individuals.

APP 10 – quality of personal information

We generally support this principle, which assists in ensuring that personal information that is collected, used and disclosed by entities is accurate, up-to-date, complete and relevant.

APP 11 – security of personal information

We generally support this principle, which requires an entity to take reasonable steps to ensure that personal information is protected from misuse, unauthorised access, loss, etc.

However, as with APP 4, we recommend that APP 11.2 could be amended to require an entity to take reasonable steps to not only destroy or de-identify personal information that

is no longer required, but also to return the information to the individual, if that is more appropriate in the circumstances (**see Recommendation 13**).

APP 12 – access to personal information

We generally support this principle, which gives members of the community an important right to request access to their personal information.

A specific timeframe is required for an organisation to respond to a request for access to personal information under APP 12.4, instead of the current proposal for a response within a "reasonable period". We consider that a specified timeframe provides more certainty for members of the public and encourages organisations to start dealing with access requests promptly (**see Recommendation 14**).

APP 12.8 specifies that when an organisation gives an individual access to their personal information the organisation must not charge an "excessive" fee. We recommend that a specified fee or other guidance on what would constitute an excessive fee be included in an accompanying Regulation or through guidance by the Privacy Commissioner. Without such guidance, members of the public could be unfairly disadvantaged by different organisations charging vastly different fees (**see Recommendation 15**).

APP 13 – correction of personal information

We broadly support this principle, which gives members of the community a right to request amendments to their personal information to ensure that the information is accurate. However, as with APP 12, we recommend that there be a specified timeframe for an organisation to respond to a request for correction of personal information instead of "within a reasonable period" (**see Recommendation 16**).

New civil penalty and changes to Privacy Commissioner's powers

We support the inclusion of a new civil penalty for serious and repeated interferences with privacy. The community expects that there will be appropriate penalties for organisations that engage in serious and repeated acts that interfere with the privacy of an individual or individuals.

We also broadly support the proposed additional powers of the Privacy Commissioner. In particular, we support the proposed provision that allows the Privacy Commissioner to accept written undertaking from entities, requiring them to comply with the *Privacy Act 1988*. We also support the proposed provision that allows the Privacy Commissioner to direct agencies to provide the Commissioner with a Privacy Impact Assessment. These and other additional powers of the Privacy Commissioner in the Bill will hopefully lead to better outcomes for the community in terms of ensuring that entities consider the privacy-related consequences of projects as soon as possible to avoid potential privacy breaches later in the process.

We hope that these submissions are of assistance to you and we thank you for the opportunity to provide our comments in relation to this important law reform initiative.

Please contact Jessica Falvey of this office on (02) 8071 7024 if you would like to discuss any of the matters that we have raised.

Yours sincerely

Dr Elizabeth Coombs
NSW Privacy Commissioner
Information and Privacy Commission