office of the privacy commissioner
new south wales

Ms Natalya Wells
Inquiry Secretary
Standing Committee on Social Policy and
Legal Affairs
Department of the House of Representatives
Parliament House
Canberra ACT 2600

By email: spla.reps@aph.gov.au

Dear Committee Members

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

Thank you for providing us with an opportunity to make a submission 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.

Our submission deals with the following issues:

1. the adequacy of the proposed Australian Privacy Principles (**APPs**);
2. whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections;
3. whether provisions relating to the use of depersonalised data are appropriate.

We have not made any comments in relation to the efficacy of the proposed measures relating to credit reporting.

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.

1 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

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

2. 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.

3. 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.

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

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

6. 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.

7. APP 6.3 should be removed from the Bill.

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 that may be issued by the Privacy Commissioner from time to time 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".

17. It is not appropriate to include defences to contraventions where systems incorporate appropriate protections but where an inadvertent disclosure nevertheless occurs. In particular, it is not appropriate to include a defence in APP 6 (use or disclosure of personal information) to the effect that if an entity has complied with APP 11 (security of personal information) then there will be no breach of APP 6 because these two principles focus on different aspects of privacy protection – one focuses on the purposes for which personal information is disclosed and the other focuses on ensuring that an entity takes reasonable steps to protect personal information.

18. Schedule 1 of the Bill should not include specific provisions relating to the use of de-identified data as it is more appropriate for the Privacy Commissioner (or other appropriate body) to issue guidance from time to time on issues such as what it means to de-identify personal information and when and how to de-identify personal information.

2 The adequacy of the proposed Australian Privacy Principles

We generally support the proposed APPs. However, in the following sections, we have made some comments and recommendations about how the APPs and associated provisions could be further improved to deliver better outcomes to the public and entities in terms of enhancing privacy protections and clarifying obligations.

2.1 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".[1] 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

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

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**).

2.2 Permitted general and health situations

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 2**).

2.3 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.[2]

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".[3] 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

---

[2] ALRC Report 108 (2008), recommendation 21-5.

[3] See National Privacy Principle 1.1 and Information Privacy Principle 1 in the Federal *Privacy Act 1988*.

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 3**).

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 4**).

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.

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.[4]

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 5**).

2.4 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.

---

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

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 6**).

2.5 APP 6 – use or disclosure of personal information

We generally support APP 6. However, in our view, the exemption provided by APP 6.3 is unnecessary. APP 6.3 allows an agency that is not an enforcement body to share "biometric information or biometric templates" with an enforcement body if the disclosure is made in line with guidelines prepared by the Privacy Commissioner.

What constitutes biometric information is very broad. It is high-level information that can be used for identification or verification of an individual. In practice, the term is broader than what most members of the public understand it to cover.

The exemptions in APP 6.2 already permit sharing of information in a very broad range of circumstances. In particular, APP 6.2(e) specifically permits disclosures where the entity reasonably believes that the disclosure is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body. We note that the proposed definition of "enforcement related activity" in item 20 of the Bill also appears to be broad.

The inclusion of the proposed exemption in APP 6.3 appears to further broaden the circumstances in which an agency can disclose personal information in the form of biometric information or biometric templates. If an agency needs to disclose this kind of information, and the disclosure would not be covered by the other provisions of APP 6, the authority to disclose such information should be dealt with in the agency's enabling legislation rather than as an exemption in APP 6.3.

We therefore recommend that the exemption in APP 6.3 be removed (**see Recommendation 7**).

2.6 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 that may be issued by the Privacy Commissioner from time to time 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.

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**).

Under the NSW privacy legislation, a NSW public sector agency does not have to comply with a particular Information Protection Principle in circumstances where an individual has expressly consented to the agency not complying with the principle.[5] However, APP 8.2(b) envisages that a person could consent either expressly or impliedly to the protections in APP 8.1 not applying to a cross border disclosure of personal information. This is of concern to us as reliance on implied consent could lead to an entity construing agreement

[5] See section 26(2) of the NSW *Privacy and Personal Information Protection Act 1998*.

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.

2.7 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**).

2.8 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**).

2.9 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**).

3 Whether defences to contraventions should extend to inadvertent disclosures where systems incorporate appropriate protections

It is not appropriate to include defences to contraventions where systems incorporate appropriate protections but where an inadvertent disclosure nevertheless occurs as this could weaken privacy protections.

The issue raised by the Committee appears to capture the interaction between APP 6 (use or disclosure of personal information) and APP 11 (security of personal information).

APP 6 focuses on ensuring that personal information is:

- disclosed for the purposes for which it was collected; and
- only disclosed for other purposes in permitted circumstances.

APP 11 focuses on ensuring that an entity takes reasonable steps to protect the personal information that it holds from, amongst other things, unauthorised disclosures. Those steps could include things such as staff training, restricting access to certain information, effective privacy and/or records management procedures, etc.

While a disclosure of personal information would normally be assessed against APP 6, it may also be assessed against APP 11 in some circumstances. For example, if an entity has not taken reasonable steps to protect personal information and this has resulted in an inappropriate disclosure, then both principles may be relevant. In these circumstances, better protection measures (such as more targeted privacy training or stricter computer security) may have prevented the inappropriate disclosure.

However, an inappropriate disclosure may not always result in a breach of APP 11. This is because an entity may have taken reasonable steps to protect the personal information but these steps may have been ignored, not followed appropriately or not properly understood, leading to the inappropriate disclosure and a breach of APP 6.

It is therefore not appropriate to include a defence in APP 6 to protect an entity from breaching this provision if they have taken reasonable steps to protect the information as required by APP 11. This is because these two principles focus on different aspects of privacy protection – one focuses on the purposes for which personal information is disclosed and the other focuses on ensuring that an entity takes reasonable steps to protect personal information. Our recommendation will leave scope to regulate those circumstances where an entity may have complied with APP 11 but has not complied with APP 6 and will ensure that strong privacy protections are retained (**see Recommendation 17**).

4 Whether provisions relating to use of depersonalised data are appropriate

It is not necessary to include specific provisions relating to the use of de-identified data because privacy principles are centred around protecting information that identifies an individual. One of the key reasons for protecting information that identifies an individual is the risk to the individual if their personal information is inappropriately dealt with. There is not the same risk associated with data that has been adequately de-identified (such as purely statistical data).

If information has been properly de-identified so that an individual cannot be re-identified in the future then the information does not need to be protected by privacy principles as it will not contain the individual's personal information.

However, privacy regulation must ensure that if an individual can be re-identified from information in the future then the entity that holds that information must deal with it in accordance with the APPs.

In our experience, the more important issue is whether an entity has the knowledge and skills to appropriately de-identify personal information so that the individual cannot be re-identified at a later date, such as through data matching or with the assistance of technology.

It is important for entities to have guidance on:

- what it means for an individual to be identified, reasonably identifiable or not reasonably identifiable;
- the kinds of circumstances where it is appropriate to de-identify personal information; and
- how to de-identify personal information.

However, we support the Australian Law Reform Commission's recommendation that the Privacy Commissioner (or other appropriate body) could give guidance on these issues.[6] We do not think it is appropriate for such guidance to be incorporated into the APPs or other provisions of the Bill because these issues depend very much on the context and will vary between entities and circumstances. It is important for there to be scope for guidance to be updated on a regular basis, if necessary, to appropriately respond to future privacy issues. If guidance was instead included in the *Privacy Act 1988*, it would limit the ability of that information to be updated and amended on a regular basis due to the stricter processes involved in amending legislation. It is also likely to further complicate the APPs and other provisions of the Bill (**see Recommendation 18**).

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.

Yours sincerely

Dr Elizabeth Coombs
NSW Privacy Commissioner
Information and Privacy Commission

[6] ALRC Report 108 (2008), recommendations 6-2, 6-3 and 28-5.