Privacy Law Consulting
AUSTRALIA

10 August 2010

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

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

Dear Sir or Madam

Submission regarding Australian Privacy Principles Exposure Draft

Please find below a submission on behalf of Privacy Law Consulting Australia regarding the Australian Privacy Principles Exposure Draft.

I thank the Committee for the extension of time in which to lodge the submission, which has enabled me to consider issues in more detail.

Throughout July 2010, I delivered seminars on the Privacy Act reforms for private sector organisations and public sector agencies. Further, since the release of the draft legislation, I have had the opportunity to discuss the proposed reforms with clients wanting to know how the reforms may impact their businesses. Many of the issues raised in this submission are an expression of concerns raised by the seminar attendees and clients.

The submission focuses on:

- concerns the reforms raise for private sector organisations and government agencies;
- practical implications which may have been unforeseen by the drafters; and
- issues regarding the technical operation and drafting of provisions.

If you would like further information in relation to, or clarification of, any of the issues raised in the submission, please do not hesitate to contact me.

Yours sincerely

Jeremy Douglas-Stewart
Principal Consultant
t (08) 8464 0876
f (08) 8278 9382

Privacy Law Consulting Australia
submission regarding
Australian Privacy Principles Exposure Draft

About Privacy Law Consulting Australia

Privacy Law Consulting Australia is a specialist privacy consultancy providing advice on privacy laws and data management practices to businesses and government agencies.

PLCA's Principal Consultant is Jeremy Douglas-Stewart. Jeremy is a legal practitioner and has specialised in advising on privacy laws and practices since 2002. Jeremy has published extensively in the field of privacy (and is author of a forthcoming *Australian Privacy Law Handbook* looseleaf service (September 2010)) and is a regular presenter of privacy training workshops for businesses, not-for-profits and government agencies.

APP 1(4)(f) and (g)

Notification of overseas disclosures

- APP 1(4)(f) and (g) require an entity to state in its privacy policy:
    - whether the entity is likely to disclose personal information to overseas recipients; and
    - if so – the countries in which such recipients are likely to be located if it is practicable to do so.
- The intention of these provisions is clear, being to inform consumers if their personal information will be sent overseas so that, if they do not wish for this to occur, they may decide not to provide their information to the entity concerned.
- For some organisations (as opposed to agencies), these obligations will be of major concern as they will be required to state information which, in effect, could reveal details about their operational arrangements and inner-workings (in particular, their outsourcing practices and the location of foreign service providers) which they may consider to be commercially confidential information. For example, many organisations that engage in business process outsourcing to overseas firms (eg outsourcing back-office functions, such as accounts or dictation transcription, or front-office functions, such as call centre operations) take steps to ensure that information about such practices is not in the public domain.
- For consumers, the effect of the provisions is questionable since the notification obligations are limited in scope – they generally only require notification of whether information is likely to be disclosed overseas and, if so, the country of the recipient. They do not, for example, require an organisation to state the name of the recipient, the purpose for which the information is disclosed or the nature of the activities of, or goods or services provided by, the recipient. Accordingly, the provisions do not result in consumers being provided with a level of information that will enable them to properly consider privacy issues associated with the overseas disclosure.
- Accordingly, APP 1(4)(f) and (g) have potentially significant consequences for organisations (in terms of having to disclose otherwise confidential information) but provide relatively little benefit for consumers. The Committee may consider it is worth reviewing whether APP 1(4)(f) and (g) have found the appropriate balance between these competing interests.

APP 3

Comments in Companion Guide re "reasonably necessary"

- The Government's *Companion Guide* to the draft APPs states in relation to APP 3 (at p 16):

  > In relation to the requirement that an entity must not collect personal information unless it is reasonably necessary for their functions or activities, this is intended to reflect two things. The first is that from the perspective of a reasonable person the function or activity is legitimate for that type of entity. The second is that the information collected is genuinely necessary to pursue that function or activity.

- The first element of this interpretation does not appear to be consistent with a literal reading of the principle.
- Further, in regards to the equivalent provision in NPP 1.1, that information be "necessary for one or more of [the relevant organisation's] functions or activities", it is generally accepted that the principle does not regulate what activities or functions an organisation may conduct (as opposed to what information is necessary for activities or functions conducted). This interpretation was confirmed by the Privacy Commissioner in her report on the private sector provisions of the Privacy Act, entitled *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, in which she stated:

  > NPP 1.1 limits the collection of personal information by an organisation to that necessary for its 'functions or activities'. The organisation itself, however, determines what its functions and activities are and the limitation on the collection of information may be seen to be illusory.

- The interpretation referred to in the *Companion Guide* would result in the Privacy Act effectively regulating, and limiting, the types of functions and activities an entity could perform or engage in (based on a test relating to whether they were reasonably legitimate for that type of entity). Such an outcome appears to be beyond the intended scope and purpose of the Act. Further, this would be inconsistent with the general demise of the doctrine of *ultra vires* in respect of corporations (which placed limitations on activities a corporation could engage in based on its objects clause in its memorandum of association) – see, for example, s 124(1) of the *Corporations Act 2001* (Cth) which generally provides that companies have the legal capacity and powers of an individual, effectively abolishing the application of the doctrine in relation to corporations established under that Act.
- It is important that any uncertainty in this regard be eliminated, otherwise entities operate under the spectre that functions or activities they perform or engage in could be challenged on privacy grounds.

APP 4(4)

Destruction of unsolicited information

- Australian Privacy Principle ("**APP**") 4(4) requires an entity to destroy or de-identify unsolicited personal information as soon as practicable after collection if the entity would not be permitted to collect it under APP 3.

- The principle doesn't indicate whether an entity is permitted to use or disclose the information for any purpose prior to destroying or de-identifying it. An organisation that has, for example, received unsolicited information in a letter from an individual requesting goods the organisation does not sell may, for example, wish to use contact details provided in the unsolicited information to notify the individual that the goods cannot be supplied. It is not clear, however, whether such use would be permitted (under APP 6) prior to destruction.
- A concern raised by agencies regarding the principle relates to handling documents that are forwarded to them in error and which, as a matter of standard practice, they would forward to the appropriate agency responsible for handling the relevant matter. For example, where letters from members of the public are forwarded by a Minister to an agency for consideration but the agency is not the correct one to handle the matter, the agency would generally seek to forward it to the appropriate agency (some agencies have indicated that, often, the documentation could be forwarded to several agencies before it arrives at the appropriate one). Agencies have indicated that this practice occurs in relation to a relatively large number of documents. It appears that APP 4 may prohibit this practice on the basis that, as soon as an agency receives any unsolicited personal information in this way, it is in effect generally obliged to destroy the information. It appears from the intention of APP 4 that the entity is not permitted to disclose the unsolicited information by forwarding it to a relevant agency (although it is not expressly stated as such).
- If APP 4 is not intended to prohibit uses or disclosures (pursuant to APP 6) of the types referred to above, this is not clear and should be clarified.

Interaction with Archives Act

- The wording of APP 4(4) establishes a circular process in regards to determining whether it is "lawful" to destroy unsolicited personal information that falls within the meaning of a "Commonwealth record" of the *Archives Act 1983* (Cth).
- In particular:
    - APP 4(4) provides that the obligation to destroy unsolicited information applies "only if it is lawful" to destroy it;
    - s 24(2) of the Archives Act provides that it is not unlawful to destroy a Commonwealth record if, among other things, it is "required by any law".
- Whilst the intention appears clear (ie unsolicited information contained in a "Commonwealth record" can be destroyed under APP 4(4) provided destruction is in accordance with the Archives Act, the qualification of "if it is lawful" in APP 4(4) creates a circular process.
- In view of the significance of the obligation for agencies to destroy information and the implications this has in terms of s 24 of the Archives Act, it would be preferable to remove this circularity by clarifying how APP 4(4) interacts with s 24 of the Archives Act.

APP 5(2)(i) and (j)

Notification of overseas disclosures and recipient countries

- APP 5(2)(i) and (j) require an entity to state in its privacy policy:
    - whether the entity is likely to disclose the personal information to overseas recipients;
    - if the entity is likely to disclose the personal information to overseas recipients – the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.
- This raises similar issues to those raised under APP 1(4)(f) and (g) (regarding notification of overseas disclosures and recipient countries in privacy collection notices) – see above.

APP 7

Complexity of structure

- APP 7(1) adopts a complex structure which establishes an equally complex matrix of data types, circumstances and requirements. For example:
    - numerous requirements are expressed in the negative (rendering them conceptually difficult to follow, particularly when combined with requirements expressed in the positive);
    - APP 7(1)(b):
        - is expressed in the form of an exemption to APP 7(1);
        - is itself subject to two pre-conditions (one of which is expressed in the negative and the other of which requires the reader to refer separately to APP 7(1)(c)); and
        - is stated to apply where APP 7(2) or (3) apply (requiring the reader to refer separately to those provisions).
- This poses issues on two levels:
    - the principle is difficult to understand, interpret and apply;
    - organisations will find it difficult to develop compliance programs and systems that can distinguish between, and manage, the matrix of data types, circumstances and requirements. This could result in, for example, organisations simply adopting "the lowest common denominator" (eg providing opt-out facilities and/or obtaining consent) in relation to all direct marketing activities, which may be unintended consequences of the principle.
- Consideration should be given to rewriting the principle to reduce its complexity.

Meaning of "direct marketing"

- Neither proposed s 15 (Definitions) of the Act nor APP 7 define the term "direct marketing".

- The Australian Direct Marketing Association's *Direct Marketing Code of Practice* (2001) defines the term for the purposes of that Code in Appendix 1 at para 3.7. The Office of the Federal Privacy Commissioner outlined what types of marketing it considers the term includes in its *Draft NPP Guidelines* (7 May 2001) at p 28. There are, however, significant variations between the definitions (with the Commissioner's view aligning more closely with the everyday meaning of the term).
- In the interests of certainty, it would be helpful if the term was defined in the Act in view of:
    - the central role this term has in determining the activities to which APP 7 applies;
    - the "catch-all" nature of the principle (as opposed to, for example, the *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth) which only apply to certain forms of direct marketing); and
    - the importance of direct marketing activities for business.

APP 7(1)(a)

Opt-out facilities and sensitive information

- APP 7(1)(a) does not require the inclusion of an opt-out facility in relation to sensitive information, but does require such a facility in a broad range of circumstances in relation to personal information generally (ie information that is not sensitive information).
- This could be perceived as being anomalous on the basis that a lower standard of protection is being provided for sensitive information than for non-sensitive information.
- However, it appears that an opt-out facility may not be required in relation to sensitive information (assuming it is not a drafting oversight) based on the fact that:
    - consent is required in *all* circumstances for use of such information for direct marketing (whereas consent for such use is required in a relatively limited set of circumstances for non-sensitive information); and
    - consent to such use can generally be revoked at any time (unless, for example, it was provided pursuant to a contractual term that cannot be amended).
- Whilst, in *theory*, consent can generally be revoked at any time, in *practice*, consumers are generally unlikely to go to the effort of revoking consent where an organisation does not have in place systems (such as an opt-out or unsubscribe facility) that enable the revocation of consent to be easily lodged, documented and actioned.
- In contrast, if an opt-out facility is provided, this facilitates consumers exercising their right to withdraw consent.
- APP 7(1)(a) should be reviewed to consider whether an opt-out facility should be required in relation to the use of sensitive information for direct marketing purposes.

APP 7(4)(b)

Circumvention of opt-out facility

- APP 7(4)(b) refers to "direct marketing by other organisations". This reference to "organisations" means that an organisation that markets on behalf of persons that are not "organisations" within the meaning of the Act (eg a small business operator) will *not* need to comply with a request to cease using or disclosing information for that purpose.
- Accordingly, the application of APP 7(4)(b) is primarily determined by whether the marketing organisation's *clients* are bound by the Act rather than whether the marketing organisation itself is bound by the Act.
- This would, for example, enable a direct marketing organisation to establish a separate corporation to market solely for clients that are not "organisations" within the meaning of the Act in order to circumvent the operation of APP 7(4)(b). This may be an unintended consequence.

APP 7(5)(c)

Notification of source of information – ambiguity

- The obligation under APP 7(5)(c) to inform an individual, upon request (pursuant to APP 7(4)(c)), of the source of information is a potentially onerous one (with significant cost implications for organisations), yet the wording of APP 7(5)(c) contains ambiguities that are likely to result in uncertainty. Any principle that potentially has significant implications (particularly in term of cost) should, to the extent possible, have any ambiguity removed to ensure that organisations are not put to unnecessary expense in the belief that a higher level of obligation exists than that which actually applies.
- APP 7(5)(c) is uncertain in two respects, as outlined below.

When duty to notify applies

- APP 7(5)(c) provides that an organisation "... must, within a reasonable period after the request is made, notify the individual of the organisation's source unless it is impracticable or unreasonable to do so." There is an element of ambiguity as to whether "impracticable or unreasonable" pertains to the "reasonable period" or the duty to "notify" such that it is unclear if APP 7(5)(c) is intended to mean:
    - where it is impracticable or unreasonable to provide a response within a reasonable period, the organisation must nevertheless provide a response after the conclusion of that period; or
    - where it is impracticable or unreasonable to notify the individual, the organisation is not required to provide a response (this appears to be the intended meaning).

Meaning of "impracticable or unreasonable"

- The level of obligation being imposed under APP 7(5)(c) depends largely on the meaning of "impracticable or unreasonable" (ie when it will be impracticable or

unreasonable to notify an individual of the organisation's source – assuming this is the intended meaning of the clause, as per above).

- Few organisations have policies, procedures or systems in place to record data sources. For example, information contained on an organisation's customer relationship management system will typically be obtained from multiple sources. However, such systems rarely record details about data sources. Accordingly, once the information is on the system, it generally is not possible to identify the source of any particular piece of information with absolute certainty.
- For many organisations, updating policies, procedures and systems to record data sources would be a logistically complex and financially burdensome process, particularly for those with large and complex information holdings and information management systems. For some organisations, it may not be possible due to logistical reasons or cost.
- To ensure that organisations are not put to unnecessary expense in the belief that a higher level of obligation exists than that which actually applies, the meaning of "impracticable or unreasonable" should be clarified (preferably in the legislation – for example, by stating what factors are to be taken into consideration in determining when notification is impracticable or unreasonable, or by providing examples in legislative notes – rather than in, for example, any guidelines to be published by the Privacy Commissioner).

Costs associated with refusing requests where it is impractical/unreasonable to notify

- As consumer awareness of any right to ask for the source of the information increases, there is potential that consumers will exercise the right on a large scale (this is suggested by the fact that it is already a relatively common question posed by consumers and, furthermore, by the high registration levels for the Do Not Call Register).
- An unintended consequence of APP 7(5)(c) for organisations may be that, even where it is impracticable or unreasonable to notify individuals of sources of information (which could be in a large number of instances in view of the issues raised above), organisations that receive a lot of requests may nevertheless need to establish systems that enable the requests to be submitted, processed and responded to in an efficient and cost-effective manner.

APP 7(6)

Interaction with Do Not Call Register Act and Spam Act

- It is unclear precisely what is meant by the phrase "apply to the extent that" in APP 7(6) since neither the *Do Not Call Register Act 2006* nor the *Spam Act 2003* regulate the *handling of personal information* per se – rather, they regulate *activities* (eg the sending of commercial emails and the making of telemarketing calls) that involve the handling of personal information. It appears that the intention is that, if one of the Acts permits an activity that necessarily involves the use or disclosure of personal information in a particular manner, APP 7 does not apply to such use or

disclosure. For example, the Spam Act permits commercial emails to be sent with consent. This suggests that an organisation will be permitted to use or disclose personal information to send such emails in accordance with the Spam Act, regardless of requirements that might otherwise apply under APP 7. The operation of APP 7(6) should be clarified in this regard.

APP 10(2)

Ensuring information used is relevant

- APP 10(2) requires an entity to, among other things, take reasonable steps to ensure that the personal information the entity uses is "relevant". For organisations, this will provide individuals with new grounds on which to lodge privacy complaints – for example, that a decision was made about them taking into account irrelevant information.
- An equivalent provision exists under IPP 9 (which prohibits an agency from using "information except for a purpose to which the information is relevant") and, to date, complaints have been lodged on these grounds (see, eg, *M v Commonwealth Agency* [2003] PrivCmrA 11 and *T v Commonwealth Agency* [2009] PrivCmrA 23). The obligation under IPP 11, however, reflects principles of procedural fairness (which generally prevent administrative decision-makers from taking into account irrelevant considerations when exercising a discretion) with which agencies are intimately familiar.
- An example of where a complaint on these grounds could arise in the context of a private sector organisation is where an organisation makes a decision to decline a service to an individual (eg an insurer refusing to provide an insurance policy to an applicant) and the individual lodges a complaint in the belief that irrelevant information about him or her was taken into account in making the decision.
- Accordingly, APP 10(2) has significant implications for private sector organisations to the extent that it establishes new grounds for a privacy complaint.
- This outcome may be the intention of the principle. On the other hand, the outcome may be an unforeseen consequence of the principle, in which case its implications for organisations may warrant further consideration.

APP 11(2)(c)

Interaction with Archives Act

- Similar issues to those raised in regards to APP 4(4) apply in relation to APP 11(2)(c) regarding circularity and interaction with the Archives Act – see above.

APP 13(1)

Meaning of "correct" irrelevant information unclear

- APP 13(1) refers to "correcting" information to ensure that it is "relevant". It is unclear what is meant by "correct" in this context since privacy issues posed by use of irrelevant information are not addressed through correction. The terminology should be amended accordingly.

APP 13(3)

Notification of correction to third parties

- The obligation under APP 13(3) regarding notification of correction to third parties raises similar issues to those raised under APP 7(5)(c) (regarding notification of source of information – see above) in the following ways:
    - for many entities, updating policies, procedures and systems to record parties to whom information is disclosed would be a logistically complex and financially burdensome process;
    - to ensure entities are not put to unnecessary expense in the belief that a higher level of obligation exists than that which actually applies, the meaning of "reasonable in the circumstances" and "impracticable" should be clarified.

Issues regarding technical operation and drafting of provisions

Technical issues regarding the operation of various provisions are outlined below.

- **APP 1(2)** – The word "inquiries" (generally being official investigations) should be "enquiries" (being general requests for information).
- **APP 3(6)** states: "This principle applies to the collection of personal information that is solicited by an entity."
    - The intention of APP 3(6) is clear (to limit the application of APP 3 to solicited collections). However, the wording is not so clear as, whilst it *includes* the application of APP 3 to solicited collections, technically, it does not *exclude* the application of APP 3 to unsolicited collections.
    - The word "only" should be inserted before "applies" to clarify this.
- **APP 8(1)** states: "... the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles ...". The overseas recipient generally will not be bound by the APPs, so could not breach the APPs. Additional wording similar to that contained in proposed s 20(1)(d) needs to be added after the wording above, eg "... if those Australian Privacy Principles applied to it".
- **APP 8(1)(b)** refers to an entity making a "disclosure":
    - to itself (eg a division of the entity in Australia making a disclosure to another of its divisions in another country); and
    - to the individual concerned.

The term “disclosure” is generally used in the context of a disclosure to a third party. Accordingly, whilst the intention of APP 8(1)(b) is clear, the terminology is technically nonsensical since an entity:

- cannot make a disclosure to itself (this amounts to an internal use);
- a provision of personal information to the individual concerned generally isn’t considered to be a disclosure (in some instances, it will be the provision of access).

The terminology should be amended accordingly.