

Legal Update

— Insurance

9 November 2009

First stage of proposed reforms to privacy law in Australia

Overview

On 14 October 2009 the Australian Government released its first stage response to the Australian Law Reform Commission's (ALRC) review of privacy law in Australia.

A copy of this response can be viewed at http://www.pmc.gov.au/privacy/alrc_docs/stage1_au_govt_response.pdf.

A copy of the ALRC's report can be viewed at <http://www.alrc.gov.au/inquiries/title/alrc108/index.html>.

The Government's first stage response focuses on establishing the foundations of the proposed law. In order to implement the proposed changes the Government will prepare exposure draft legislation to be released in early 2010 for further consultation.

In summary, the Government is proposing to:

- create a harmonised set of Privacy Principles which will replace the separate sets of public and private sector principles at the federal level, untangling red tape and marking a significant step on the road to national consistency;

- redraft and update the Privacy Act to make the law clearer and easier to comply with;
- create a comprehensive credit reporting framework which will improve individual credit assessments, complimenting the Government's reforms to responsible lending practices;
- improve health sector information flows, and give individuals new rights to control their health records, contributing to better health service delivery;
- require the public and private sector to ensure the right to privacy will continue to be protected if personal information is sent overseas; and
- strengthen the Privacy Commissioner's powers to conduct investigations, resolve complaints and promote compliance, thereby contributing to more effective and stronger protection of the right to privacy.

In this article we will only deal with the proposed Uniform Privacy Principles and the credit reporting framework as these are the most significant proposals included in the Government's first stage response.

Privacy Principles

One of the most significant proposals is the enactment of a single set of Privacy Principles to protect personal information held by both Australian Government agencies (agencies) and relevant businesses in the private sector (organisations).

This harmonised set of Privacy Principles (which the ALRC referred to as "Uniform Privacy Principles" (UPPs)) will replace the existing Privacy Principles and National Privacy Principles (NPPs). Apart from the fact that agencies are now caught by them, the proposed UPPs appear to be very similar to the existing NPPs, but there are some differences which may impact on how organisations deal with personal information.

We summarise below the key terms of the proposed UPPs:

Anonymity and Pseudonymity principle

This proposed UPP reflects what is provided for in NPP 8 (Anonymity).

It is proposed that this principle should require an agency or organisation to give individuals the clear option to interact anonymously or pseudonymously, where it is lawful and practicable in the circumstances to do so.

Collection principle

This UPP appears to follow the provisions of NPP 1 (Collection). However, it is proposed that in addition this UPP should provide that, where an agency or organisation receives unsolicited personal information, it must either:

- (a) destroy the information (if lawful and reasonable to do so) as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
- (b) comply with all relevant provisions in the model UPPs that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

It is also proposed that the collection principle should set out the requirements of agencies and organisations in relation to the collection of personal information that is defined as "sensitive information" for the purposes of the Privacy Act. This is currently provided for in NPP 10 (Sensitive information).

Notification principle

The notification principle will provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify or otherwise ensure that the individual is aware of the:

- (a) fact and circumstances of collection in situations where the individual may not be aware that his or her personal information has been collected;

- (b) identity and contact details of the agency or organisation;
 - (c) rights of access to, and correction of, personal information provided by these principles;
 - (d) purposes for which the information has been collected;
 - (e) main consequences of not providing information;
 - (f) actual, or types of, agencies, organisations, entities or persons to whom the agency or organisation usually discloses personal information of the kind collected;
 - (g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and
 - (h) fact, where applicable, that the collection is required or authorised by or under law.
- (c) the steps individuals may take to access and correct personal information about them held by the agency or organisation; and
 - (d) the avenues of complaint available to individuals in the event that they have a privacy complaint.

In addition to the above is it also recommended by the Government that this UPP should require agencies and organisations to take reasonable steps, having regard to the circumstances of the agency or organisation, to develop and implement internal policies and practices that enable compliance with the Privacy Principles. These policies and practices could include:

Openness principle

Under this UPP agencies and organisations are required to clearly set out express policies on their handling of personal information in a Privacy Policy, including how they collect, hold, use and disclose personal information. The Privacy Policy should also include:

- (a) the type of personal information the agency or organisation holds;
- (b) the purposes for which personal information is held;

- (a) training staff and communicating to staff information about the agency or organisation's policies and practices;
- (b) establishing procedures to receive and respond to complaints and inquiries;
- (c) developing information to explain the agency or organisation's policies and procedures; and
- (d) establishing procedures to identify and manage privacy risks and compliance issues, including designing and implementing systems or infrastructure for the collection and handling of personal information by the agency or organisation.

This UPP appears to amend NPP 5 (Openness) in a number of ways which will call for organisations to review (and possibly amend) their existing Privacy Policies to ensure that they are compliant with this UPP.

Use and disclosure principle

This UPP will set out the requirements imposed on agencies and organisations in respect of the use and disclosure of personal information for a purpose other than the primary purpose of collection.

NPP 2 (Use and disclosure) currently provides for a number of exceptions permitting an organisation to use or disclose an individual's personal information for a purpose other than the primary purpose of collection, which are proposed to be mirrored in this UPP.

However, the Government recommended that, in addition to the existing exceptions provided for in NPP 2, this UPP should also have the following exceptions:

- (a) where the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process; and
- (b) where the personal information may be used for research purposes (subject to the relevant provisions of the Privacy Act).

Direct marketing principle

It is proposed that a UPP should regulate direct marketing by organisations in a discrete privacy principle, separate from the Use and Disclosure UPP, called the Direct Marketing UPP.

This UPP will apply regardless of whether an organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing.

The principle will also distinguish between direct marketing to individuals who are existing customers and direct marketing to individuals who are not existing customers.

The ALRC recommended that the Direct marketing UPP should set out the generally applicable requirements for organisations engaged in the practice of direct marketing.

The Government proposed that the general requirements of the direct marketing UPP should be displaced by more specific legislation that regulates the handling of personal information for direct marketing (e.g. the Do Not Call Register Act 2006 (Cth)) .

Under this UPP organisations may only use or disclose personal information about an individual who is an existing customer for the purpose of direct marketing where:

- (a) the individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing;
- (b) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications;

- (c) either:
 - (i) the individual has consented; or
 - (ii) the information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;
- (d) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays, a notice advising the individual that he or she may express a wish not to receive any direct marketing communications; and
- (e) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications.

Data quality principle

This UPP is similar to NPP 3 (Data Quality), but it has an additional requirement that agencies and organisations must take reasonable steps to make certain that the personal information it collects is relevant.

Data security

This UPP appears to be similar to NPP 4 (Data Security). However, it is proposed that the UPP should require an agency or organisation to take reasonable steps to destroy or render non-identifiable personal information if:

- (a) it is no longer needed for any purpose for which it can be used or disclosed under the model UPPs; and
- (b) retention is not required or authorised by or under law.

Access and correction principle

This UPP will reflect NPP 6 (Access and Correction), but will equally apply to agencies.

Accordingly, it is proposed that this UPP should provide that if an agency holds personal information about an individual, the individual concerned is entitled to have access to that personal information, except to the extent that the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents.

In addition, it is proposed that the Access and Correction UPP should provide that, if an individual seeks to have personal information corrected under the principle, an agency or organisation must take such steps, if any, as are reasonable to:

- (a) correct the personal information so that, with reference to a purpose for which the information is held, it is accurate, relevant, up-to-date, complete and not misleading; and

- (b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

It is also proposed that the existing NPP 6.6 be amended to provide that an agency or organisation must, in the following circumstances, if requested to do so by the individual concerned, take reasonable steps to 'associate' with the record a statement of the correction sought:

- (a) if the agency or organisation that holds personal information is not willing to correct personal information in accordance with a request by the individual concerned; and
- (b) where the personal information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.

This UPP will also contain a provision that obligates an organisation or agency to:

- (a) respond within a reasonable period of time to a request from an individual for access to his or her personal information held by the agency or organisation; and
- (b) provide access in the manner requested by the individual, where reasonable and practicable.

Under this UPP an organisation or agency should notify an individual of the potential avenues for complaint when an agency or organisation denies a request for access, or refuses to correct personal information.

Identifiers principle

This UPP will in essence follow NPP 7 (Identifiers), but the following additions to NPP 7 are proposed:

- (a) the Identifiers UPP will include an exception for the adoption, use or disclosure by prescribed organisations of prescribed identifiers in prescribed circumstances (to be set out in regulations under the Privacy Act);
- (b) the identifiers UPP will define 'identifier' inclusively to mean a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:
 - (i) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or
 - (ii) is determined to be an identifier by the Privacy Commissioner,

however, an individual's name or a company's Australian Business Number is not an identifier.

Cross-border data flows principle

It is proposed that the Cross-border data flows UPP will provide that, if an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia or an external territory, the agency or organisation remains accountable for that personal information, unless the:

- (a) agency or organisation reasonably believes that the recipient of the information is subject to obligations to uphold privacy protections substantially similar to the Privacy Principles, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model UPPs;
- (b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
- (c) agency or organisation is required or authorised by or under law to transfer the personal information.

In contrast to NPP 9 (Trans-border data flows) organisations and agencies will remain accountable for the personal information unless the above applies.

Credit reporting framework

In its response to the ALRC report the Government recognised that Part IIIA of the Privacy Act (credit reporting provisions) is overly complex and prescriptive. Accordingly it is proposed by the Government to redraft this part in order to provide for a more user-friendly regulation of credit reporting in line with the ALRC's recommendations.

Under this reform, credit providers and credit reporting agencies that are small businesses will be required to comply with the Privacy Act. This will ensure that all credit providers and credit reporting agencies are subject both to the UPPs and the credit reporting provisions in the Privacy Act.

In its response to the ALRC's report the Government recommended that the definition of 'credit' in the Privacy Act should be brought in line with the definition of 'credit' in the proposed National Consumer Credit Protection Bill 2009 (NCCP Bill) so as to include credit provided to purchase residential investment properties.

Another significant proposal is the amendment of the definition of 'credit reporting information' in the Privacy Act to read as follows:

"personal information that is:

- (a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or

(b) held by a credit provider and

(i) has been prepared by a credit reporting agency; and

(ii) is used, has been used or has the capacity to be used in establishing an individual's eligibility to credit."

In this regard it is also proposed that the Privacy Act should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information and provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose such credit reporting information.

It is proposed by the Government that the 'dominant purpose' test be removed from the definition of 'credit reporting business' as it is concerned that any relevant business, regardless of whether credit reporting is a large or small component of its activities, should be covered by the credit reporting provisions.

As part of this reform it is proposed that industry participants, together with the Office of the Privacy Commissioner, draft a new binding industry code of conduct which would deal with a range of operational matters relevant to compliance, which include:

- (a) the timelines for the reporting of credit reporting information;
- (b) the calculation of overdue payments for credit reporting purposes;
- (c) obligations to prevent the multiple listing of the same debt;
- (d) the updating of credit information; and
- (e) the linking of credit reporting information relating to individuals who may or may not be the same individual.

With regards to penalties, it is recommended that the Privacy Act should be amended to remove the credit reporting offences and allow a civil penalty to be imposed instead.

Mark Radford
Partner

T: 02 8281 4442

E: mar@cbp.com.au