Privacy

Editor: Normann Witzleb

EXPOSURE DRAFT OF THE NEW AUSTRALIAN PRIVACY PRINCIPLES – THE FIRST STAGE OF REFORMS TO THE PRIVACY ACT 1988 (CTH)

Despite losing majority support in the last federal election, the Labor government continues to pursue its agenda of privacy law reform. In October 2009, the Labor government released its first stage response to the Australian Law Reform Commission (ALRC) landmark report, *For Your Information: Australian Privacy Law and Practice*. In that report, the ALRC had recommended a complete overhaul of the *Privacy Act 1988* (Cth) to make Australia's privacy laws stronger, easier to understand and fit for the 21st century. In the first stage response, the government outlined that, due to the sheer number of recommendations made, it would need to implement its reform in stages. In June 2010, the Labor government referred an Exposure Draft of the new Australian Privacy Principles (APP) to the Senate Standing Committee on Finance and Public Administration for consultation. The Senate inquiry into the exposure draft and a draft companion guide[1] lapsed with the dissolution of Parliament. After the Senate re-adopted the inquiry, the Committee will now report on 1 July 2011.

This note will provide an overview of the proposed new privacy principles and how the amendments are likely to affect business organisations. The APP will be supplemented by new provisions on credit reporting and on health privacy as well as provisions that strengthen the powers for the Privacy Commissioner (whose office has, from 1 November 2011, been incorporated into the new Office of the Australian Information Commissioner). Some of the most contentious issues raised by the ALRC report have been deferred until the second stage of the implementation process. These issues include:

- the exemptions from the *Privacy Act*, in particular for small businesses and employee records;
- the introduction of a statutory cause of action for serious invasion of privacy;
- notification requirements for serious breaches of data protection;
- privacy and decision-making issues for children and authorised representatives; and
- handling of personal information under the *Telecommunications Act 1997*.

The introduction of a statutory cause of action for serious invasions of privacy has recently also been recommended by the NSW and Victorian Law Reform Commissions. The second stage amendments will be subject to further consultation once the first stage has been progressed. On completion, all component parts of the reform package will be consolidated in a new *Privacy Act*.

The current draft of the APP has received a mixed response. In submissions to the Senate Standing Committee, the Federal, NSW and Victorian privacy commissioners have welcomed the creation of a single, coherent and modern set of principles that may also provide a template for privacy law reform at State and Territory level. However, in some areas the government proposes to water down recommendations made by the ALRC, thereby giving in to agency and business demands for weaker privacy obligations. Many of the submissions also call for the principles to be drafted in simpler language and a more accessible style. In their current form, the APP make it unnecessarily difficult for agencies and organisations to comply with their privacy obligations and for individuals to readily understand their rights.

The proposed new privacy principles will form the centrepiece of the new *Privacy Act*. It is a key aim of the reform to consolidate the two existing sets of privacy principles at federal level into a single set. The APP will apply to both the public and private sector, replacing the Information Privacy Principles (the IPP apply to Commonwealth agencies) and the National Privacy Principles (the NPP apply to specified private organisations) currently contained in the *Privacy Act 1988* (Cth). Where a

[1] The *Exposure Draft and Companion Guide* are available at http://www.aph.gov.au/senate/committee/fapa_ctte/priv_exp_drafts/index.htm viewed 24 January 2011.

principle applies to agencies as well as organisations, the draft legislation uses the new term "entity". Similar to the current law and in line with the recommendations of the ALRC, the new *Privacy Act* adopts a principles-based and technology-neutral approach to regulating privacy. The proposed APP therefore deal with the collection, holding, use, disclosure, access to and correction of personal information at a relatively broad level. Many of the principles employ general terms such as "reasonably necessary", "reasonably believes", "unless impracticable or unreasonable" etc, which require further definition for specific contexts of application. It is expected that the Office of the Privacy Commissioner will develop and publish more detailed guidance in the form of guidelines, determinations and fact sheets that assist with the practical application of the APP. While the principles are now unified, the draft legislation takes the interests of government agencies into account particularly through specific exceptions to the principles. The majority of principles follow on from the NPP and IPP but there are also some principles without predecessor in the current law. New principles include a requirement for open and transparent management of personal information, more specific regulation of direct marketing activities, restrictions on the use of government-related identifiers by the private sector as well as a new regime for cross-border disclosure of personal information.

The new APP 1 requires entities to manage personal information openly and transparently. This principle is intended to ensure that entities plan how they will handle personal information, and design their information management systems with privacy in mind, before they collect and use personal information. The significance of putting effective frameworks for data handling in place has recently also been emphasised in other contexts, eg the reform of the secrecy laws.[2] Under APP 1, entities must take reasonable steps to develop systems that ensure compliance with the APP and must adopt a clear and up-to-date privacy policy. Similar requirements exist under current law but the APP gives these obligations more prominence, thereby following international trends that encourage pro-active information management and protecting "privacy by design". Publicly available privacy policies must in future be more encompassing and contain information on how individuals can access and seek correction of their personal information, or make a complaint about a privacy interference, and provide details on whether their personal information is likely to be disclosed to overseas recipients and to where it may be disclosed.

APP 2 provides that individuals must be given the option not to identify themselves, or to use a pseudonym, when interacting with entities unless this anonymity or pseudonymity are not lawful or not practicable. This new privacy principle rightly emphasises that entities should consider whether the collection of identifying information is necessary for the provision of the service. It is unlikely that the new principle will cause a great additional burden to business because the current NPP 8 already provides a limited right for an individual to transact anonymously with organisations.

APP 2 reinforces the requirement of APP 3, dealing with the collection of solicited information. APP 3 requires that entities do not collect personal information unless the information is "reasonably necessary for, or directly related to", one or more of the entity's function or activities. This new formulation appears to merge the current IPP 1 and NPP 1 but, by doing so, sets a lower bar than NPP 1, which requires the collection to be "necessary" for an entity's functions. It also differs from the 2009 Government Response, which had accepted the ALRC recommendation to adopt the NPP 1 requirement of "necessity". It has therefore been roundly criticised in submissions to the Senate Inquiry. In relation to sensitive information (which includes information that relates to an individual's race or ethnic origin, political opinions and associations, religious or philosophical beliefs, health, sexual orientation or practices, as well as genetic and biometric information), APP 3 requires additionally that the individual consents to the collection of the information unless an exception applies. However, the protection of sensitive information has become likewise become weaker than under present law, in particular through an expansion of the circumstances in which sensitive information can be collected without the individual's consent. Oddly, the current draft also appears to allow these exceptions to override the requirement that the information is necessary for, or directly related to, a function or activity, thereby allowing collection of sensitive information in a wider set of

[2] Australian Law Reform Commission, *Secrecy Laws and Open Government in Australia*, Report 112 (2009).

circumstances than non-sensitive information. As under the current NPP, information must be collected by lawful and fair means as well as, unless unreasonable or impracticable to do so, directly from the individual.

The receipt of unsolicited personal information will in future be dealt with in a separate principle. Under APP 4, an entity that receives personal information without having taken active steps to collect it, must decide whether it could have collected the information under APP 3. If it could have done so, the APP will apply as if the information had been collected. If not, the entity is obliged to take all lawful and reasonable steps to destroy the information or to ensure that it is no longer personal information, eg by de-identifying it. This new principle clarifies that unsolicited information does not fall outside the scope of the *Privacy Act*. It also ensures that an entity which is obliged, or decides, to retain it must then comply with all of the privacy principles in respect of that information.

The notification principle in APP 5 seeks to ensure that individuals are informed about how and why their personal information is, or will be, collected and how it will be dealt with. Apart from the matters currently listed in NPP 1.3 and 1.5, businesses will need to review their existing privacy notices to include further information, including:

- notification about the circumstances of collection, if information has not been collected directly from the individual;
- the name of the law that requires or authorises the collection;
- references to the information in the entity's privacy policy on access and complaints regimes; and
- notification whether information is likely to be disclosed to overseas recipients and, if practicable, also specify the countries in which such recipient are located.

These requirements are likely to promote greater transparency about data handling practices and thereby allow individuals to exercise a greater degree of control.

APP 6 sets the parameters for the use and disclosure of personal information. The general rule is that information may be used or disclosed for the primary purpose for which it has been collected, for related secondary purposes if the individual would have reasonably expected such use or disclosure and for any other secondary purpose if the individual has consented. Exceptions to the general rule relate to circumstances where the public interest in use or disclosure outweighs the interest in privacy.

The use and disclosure provisions in APP 6 also do not apply to direct marketing, which is now regulated in a separate privacy principle (APP 7). Direct marketing activities have come under increasing scrutiny and, if intrusive, cause great community concern. The new APP 7 will only apply to direct marketing that is not governed by the *Spam Act 2003* (Cth) or the *Do Not Call Register Act 2006* (Cth), thereby excluding electronic messaging and telemarketing. The exposure draft of APP 7 is broadly modeled on the ALRC recommendations but does not adopt the proposed distinction between existing customers and prospective customers. Instead, it distinguishes between three scenarios that impose differing privacy obligations on the direct marketing of organisations (but not agencies). Sensitive information can generally not be used or disclosed for direct marketing without the individual's consent. Where the information used is non-sensitive, the draft legislation distinguishes two situations. First, where the organisation has collected the information from the individual and the individual would reasonably expect it to be used or disclosed for direct marketing, the information may be used for that purpose unless the individual has been given an easy means of opting out and has chosen to opt out. This scenario will apply mainly to existing customers of an organisation. Secondly, somewhat more onerous obligations apply where the organisation has obtained the individual's information indirectly or direct marketing would not be a reasonably expected use of the personal information. In these cases, direct marketing requires the individual's consent unless obtaining consent is impracticable. Furthermore, the organisation must draw to the individual's attention that they have the opportunity to opt out with each direct marketing communication.

The effect of APP 7 is to give the requirement for consent greater practical relevance than under current law and to make it easier for individuals to opt out of unwelcome direct marketing. Under APP 7, opt-outs need to be given effect within a reasonable time and free of charge. In future, individuals will also have the right to ask direct marketing organisations for the source of the personal information they use or disclose. However, the practical effect of this right is limited because organisations can

refuse to provide the sources of their information if it is impracticable or unreasonable to do so. The government has also abandoned the special protections recommended by the ALRC for children under the age of 15. As with a number of other provisions, the complex language used in this draft APP makes it unnecessarily difficult to understand.

APP 8 deals with cross-border disclosure of personal information. In an era, where it is becoming increasingly common for business organisations as well governments to send personal data of their customers, suppliers, employees or citizens overseas, the security of such data transfers is a great concern. APP 8 implements the so-called "accountability principle" that is also part of the Asia-Pacific Economic Cooperation (APEC) Privacy Framework. Under this principle, an Australian entity will, in principle, remain liable when it discloses personal information to a recipient outside Australia and must take reasonable steps to ensure that the overseas recipient complies with the APP in relation to the information. This will usually be done in the form of a contractual arrangement between the Australian exporter and the foreign data handler. Under s 20 of the draft *Privacy Act*, acts and practices of the overseas recipient will be taken to be those of the disclosing Australian entity and the entity will remain liable if the overseas act or practice fails to comply with the APP (other than APP 1).

However, APP 8 creates exceptions that severely limit this accountability. One exception arises when the disclosing entity reasonably believes that the privacy obligations applying to the overseas entity by virtue of law or a binding scheme are overall substantially similar or better than the protections provided by the APP and that the individual has access to overseas enforcement mechanisms. (In contrast to current law, a contractual agreement between the entity and the foreign data handler to respect Australian privacy standards no longer provides an exception from the general accountability obligations.) A further exception arises when the individual consents to the cross-border disclosure after having been expressly informed that the organisation will not take reasonable steps to ensure that the data handling overseas complies with the APP protection. Both exceptions, in effect, adopt recommendations of the ALRC but remain highly contentious. In relation to the first exception, it seems inappropriate to require no more than a reasonable belief that comparable protections exist abroad, rather than to adopt an objective standard (as is the case, eg under the relevant European Union (EU) directive). This effectively places the risk that protections in place overseas fall short of Australian standards on the individual, rather than on the entity that decides to outsource some of its information handling to an overseas organisation. In relation to the second exception, the draft legislation requires that the entity merely expressly disclose that it will not take reasonable steps to safeguard the information but does not require the express consent of the affected individual. This may have the consequence that an individual loses the right to hold the entity liable through implied or bundled consent, or where the disclosure is hidden in a lengthy privacy statement. Overall, it seems that APP 8 will do little to substantially improve on the weak protections currently in place for cross-border data transfers. However, it is envisaged that the Privacy Commissioner will provide further guidance on important issues arising from the new regime, including which issues should be addressed in a contractual agreement with an overseas recipient of personal information and which overseas laws and binding schemes offer a comparable level of protection.

APP 9 concerns the adoption of so-called government related identifiers, ie numbers, letters or symbols used by government agencies to identify an individual, such as a person's Medicare number. APP 9 provides that an organisation must generally not adopt a government-related identifier as identifier of the individual for its own purposes. The use of government-related identifiers by organisations is undesirable because it increases the scope and potential for data matching between agencies and organisations. However, certain exceptions apply to the general prohibition on the use of government identifiers, eg to verify the individual's identity or where it is required or authorised by law.

Under APP 10, entities must take reasonable steps to ensure that personal information they collect, disclose or use is up-to-date, accurate, complete and relevant. This principles correlates with APP 13, under which entities must take reasonable steps to correct information when they become aware, either on their own or after a request for correction, that information is no longer correct. APP 11 concerns the security of personal information and imposes an obligation to protect information

against loss, misuse, unauthorised access or modification. If an entity no longer needs the personal information, it is obliged to destroy it or to de-identify the information. All these principles largely mirror the existing IPP and NPP provisions and are therefore not likely to require major changes to current practices. APP 12 provides that entities must, on request, generally provide access to the personal information they hold about an individual and also specifies when exceptions to this principle apply. Business organisations will be obliged to respond to such requests within a reasonable period of time and must not charge an excessive amount for providing access. For the existing legislation, the Office of the Federal Privacy Commissioner has issued guidance that access should be granted within 15 days in straightforward cases and within 30 days in more complicated cases.

In summary, the forthcoming APP will provide a new era for privacy protection in Australia. For the first time, the principles that apply to public sector "agencies" and private sector "organisations" will be collated within the same set of principles. The draft APP appear to be more closely modeled on the existing private sector provisions than on the principles applying to government, which makes it likely than government agencies will be required to make greater adjustments to their practices than business organisations. However, there are numerous amendments that will also make it necessary for businesses to thoroughly review their processes and documentation. This includes a revision of the privacy policies and privacy notices currently in use because the new APP requires additional information to be provided to individuals. It is likely that the unified principles will make privacy protection more effective even though at present the inadequate drafting makes the principles overall still less than user friendly.

Dr Normann Witzleb
Faculty of Law, Monash University