JONES DAY

MAY 2014

COMMENTARY

Significant Changes to Australian Privacy Laws

Several major changes to Australia's privacy laws took effect on March 12, 2014. Amendments to the *Privacy Act 1988* (Cth) ("Privacy Act") introduced by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) included changes to the enforcement powers of the information commissioner, changes to credit reporting laws recognizing external dispute resolution schemes, provision for the information commissioner to develop and impose binding Privacy Codes, and, most importantly, the adoption of 13 new Australian Privacy Principles ("APPs").

The new APPs replace the former private sector National Privacy Principles ("NPPs") that applied to "organizations" and the public sector Information Privacy Principles that applied to "agencies." The APPs now apply generally to "APP entities" (defined to include private sector organizations and public sector agencies), with some specific obligations that apply to organizations only and some that apply to agencies only. This *Commentary* focuses on the changes introduced through the adoption of the new APPs. The key changes introduced by the APPs that affect private sector organizations conducting business in Australia are outlined below.

Application of the Privacy Act, APPs, and Credit Reporting Code to Foreign Entities

Although the new Privacy Act generally retains the same provisions relating to foreign corporations, the Privacy Act now provides that the Privacy Act, the APPs, and the new Credit Reporting Code will apply generally to those organizations that have an "Australian link." Organizations with an "Australian link" include partnerships, trusts, and bodies corporate formed or incorporated in Australia, and unincorporated associations that have their central management and control in Australia, with an annual turnover of greater than AUD3 million (when combined with the turnover of all of their related entities). In addition, organizations and small business operators (namely, those entities with an annual turnover of less than AUD3 million) formed or incorporated outside of Australia can also have an "Australian link."

An entity that is located outside Australia, is not formed or incorporated in Australia, and has no physical presence in Australia will have an "Australian link" if the entity collects personal information from individuals who are physically present in Australia as part of the carrying on of business in Australia (for example,

the entity's website offers goods or services to individuals in Australia, and the entity collects such individuals' personal information in the course of doing so). Accordingly, the changes have broadened the scope of coverage of the Privacy Act, in particular capturing foreign "e-tailers" targeting Australian consumers (including small business operators with an annual turnover of less than AUD3 million).

Privacy Policy and APP Compliance Procedures

APP 1 introduces further requirements concerning information that must be included in privacy policies, which all organizations with an "Australian link" and that collect personal information must have in place. Organizations must now ensure that their privacy policies include information on how an individual can access and seek the correction of their personal information, how individuals may complain about a breach of the APPs, how the organization deals with complaints, and whether the organization is likely to disclose personal information to overseas recipients (and, if practicable, the countries in which the overseas recipients are likely to be located).

The new APP 1 additionally requires organizations to take reasonable steps to implement practices, procedures, and systems relating to the organization's functions or activities to ensure that the organization complies with the APPs and any applicable APP codes, and enables the organization to deal with individuals' inquiries or complaints.

Collection of Solicited and Unsolicited Information

The APPs create a new distinction between an organization's obligations in relation to the receipt of unsolicited or solicited personal information. An organization "solicits" personal information if it requests (namely, takes active steps) another agency, organization, individual, or small business operator to provide personal information.

However, if the organization has solicited personal information, the organization must not collect personal information unless it is "'reasonably necessary" for one of the organization's functions or activities. If the organization receives unsolicited personal information and the organization determines that it could not have collected the personal information under the requirements contained in APP 3 regarding the collection of solicited personal information, the organization must, if it is lawful and reasonable to do so and the information is not contained in a Commonwealth record, destroy or de-identify the unsolicited information as soon as is practicable.

Notification of Collection of Personal Information

The new APPs generally retain the notification requirements under the former NPPs. However, under APP 5.2, if organizations have collected an individual's personal information from another entity or individual, or the individual may not be aware that the organization has collected his or her personal information, organizations will be required to take reasonable steps to notify the individual, or ensure that the individual is made aware that the organization collects or has collected his or her personal information and the circumstances of the collection. This notification is to occur at or before the time of collection or, if not practicable, as soon as practicable after collection.

The APP Guidelines state that the concept of "collection" of information is to be applied broadly and includes "gathering, acquiring or obtaining personal information from any source and by any means." Thus, under the new APPs, if an organization "receives" personal information from another entity that the organization is acquiring as part of an asset sale or share sale, the recipient of the personal information will have an obligation to either notify the data subject or ensure that the data subject is otherwise notified of the collection of information.

Direct Marketing Rules

Previously, the requirements for the use of personal information for direct marketing were contained in NPP 2, and direct marketing was considered a secondary purpose of collection. The requirements for using personal information for direct marketing are now directly addressed in a separate new APP 7. There is now a general prohibition against using or disclosing personal information for the purpose of direct marketing; however, there are exceptions to this prohibition if an organization meets certain requirements.

If the organization has collected the personal information from the individual, the organization may use or disclose the collected personal information for the purpose of direct marketing if:

- The individual would reasonably expect that his or her personal information would be used or disclosed for the purpose of direct marketing;
- The organization has provided simple means by which the individual can request not to receive direct marketing; and
- The individual has not requested that the organization stop sending direct marketing.

However, if an organization has not collected the information from the data subject and has collected the information from a third party, or an individual would not reasonably expect that his or her personal information would be used for direct marketing, the organization may use or disclose the personal information for the purpose of direct marketing only if:

- The individual has consented to the use or disclosure of his or her personal information for the purpose of direct marketing, or it is impracticable to seek the consent of individuals;
- The organization has provided simple means by which the individual can request not to receive direct marketing;
- The individual has not requested that the organization stop sending direct marketing; and
- The organization includes in each direct marketing communication a prominent statement that informs the individual that he or she may request not to receive direct marketing.

Organizations are also required to comply with requests made by individuals to not disclose their personal information to other organizations for the purpose of direct marketing and request not to receive direct marketing communications from the organization. If such a request has been made, organizations are required to comply with the request within a reasonable time period and without cost to the individual. Individuals may also request that an organization provide its source for the individuals' personal information; however, organizations are not required to comply with this request if it is impracticable or unreasonable to comply with the request to disclose the source of personal information.

The new direct marketing requirements found in APP 7 do not affect the operation of the *Spam Act 2003* (Cth) nor the *Do Not Call Register Act 2006* (Cth), which continue to apply.

Cross-Border Data Transfer

The new APP 8 requires entities to take reasonable steps prior to disclosure of personal information to overseas recipients to ensure that the overseas recipients do not breach the APPs. Such reasonable steps would include having agreements in place with overseas group entities and third-party service providers to ensure their compliance with the APPs in dealing with the disclosed personal information.

However, there are certain exceptions to the requirement to take reasonable steps to ensure that overseas recipients do not breach the APPs. These exceptions include:

- The disclosing entity reasonably believes that the overseas recipient is subject to a legal system that has the effect of protecting an individual's information in a substantially similar way to the APPs, and the individual is able to take action to enforce the protection of his or her personal information in that legal system; or
- Informing the individual that if he or she consents to the disclosure of the personal information, the entity will not be required to take reasonable steps to ensure that the overseas recipients do not breach the APPs, and the individual consents to this disclosure of his or her information in such circumstances.

The newly introduced section 16C of the Privacy Act also makes disclosing entities accountable, in certain circumstances, for acts of, or practices engaged in by, overseas recipients that are in breach of the APPs. To ensure compliance with the cross-border disclosure of personal information obligations, entities should review, and possibly amend, the current agreements that they have with overseas recipients of personal information such that the overseas recipients agree to comply with the APPs. Otherwise, entities should conduct a review of the relevant privacy laws that bind overseas recipients and determine whether these privacy laws contain similar requirements to those found in the APPs.

Implications for Businesses

Both local Australian and foreign entities carrying on business in Australia should conduct a careful review of their privacy policies, direct marketing communications, and

arrangements with overseas recipients of personal information and make any changes necessary to such policies and communications to ensure compliance with the new APPs. Entities should also develop practices, procedures, and systems to ensure operational compliance with the new APPs and to deal with inquiries or complaints relating to the use or disclosure of personal information. This could include the development of an internal privacy compliance guide, the provision of training key staff involved in ensuring ongoing compliance with the Privacy Act in Australia, and conducting regular privacy audits.

Jones Day is currently assisting a number of local and foreign clients with the update of their local Australian privacy policies to ensure compliance with the new APPs and advising on the new obligations imposed on organizations under the APPs and would be happy to assist with the review of your existing privacy policies and practices, procedures, and systems.

Notification of Serious Data Breaches

In addition to the recently introduced Privacy Act changes, the *Privacy Amendment (Privacy Alerts) Bill 2014* was recently reintroduced into the Australian Parliament's upper house on March 20. The bill was previously introduced on May 29, 2013, but due to several changes in the leadership of the previous government, it failed to pass through Parliament. In its current form, the bill requires organizations to notify the information commissioner of serious data breaches in relation to personal, credit reporting, credit eligibility, or tax file number information.

A serious data breach will have occurred if:

- An entity breaches the requirements in APP 11 relating to the security of personal information;
- There is unauthorized access to, disclosure of, or loss of personal information; and
- The access, disclosure, or loss of personal information results in a real risk of serious harm to any of the individuals to whom the personal information relates.

This will also extend to cover serious data breaches affecting overseas recipients of personal information as if the breach was caused by the Australian organization. Significant fines and other penalties may be imposed on individuals and corporations by the information commissioner under its new enforcement powers where they fail to comply with the data breach notification requirements.

If the bill is passed, entities will be required to prepare a statement to the information commissioner including a description of the serious data breach, the types of personal information concerned, and recommendations about the steps individuals should take in response to the serious data breach. Entities will then be further required to take reasonable steps to notify individuals significantly affected by the serious data breach. This notification will include the contents of the entity's statement regarding the data breach and the publication of a copy of the statement on the entity's website, as well as in a newspaper in each state of Australia.

If the bill is passed by Parliament, entities should be aware that they will be subject to a mandatory data breach notification requirement that may further empower the information commissioner to investigate and prosecute serious data breaches. The bill has passed through the lower house of Parliament and is currently in the upper house waiting its assent, which cannot occur until after the next senate committee meeting in July.

Lawyer Contact

For further information, please contact your principal Firm representative or the lawyer listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com.

Adam Salter
Sydney
+61.2.8272.0514
asalter@jonesday.com

Nicola Walker of the Sydney Office assisted in the preparation of this Commentary.