fact sheet

July 2013

NUMBER 32

Australian Privacy Principle 6 – Use and disclosure

Currently, the *Privacy Act 1988* applies different but substantively similar limits on the use of personal information by Commonwealth agencies (Information Privacy Principle (IPP) 10) and the disclosure of personal information by Commonwealth agencies (IPP 11).

Australian Privacy Principle 6 (APP 6) will combine these requirements relating to use and disclosure of personal information by Commonwealth agencies into a single principle, simplifying compliance obligations as well as introducing new exceptions to prohibitions on use and disclosure.

This fact sheet provides an overview of the current requirements relating to use and disclosure of personal information under IPP 10 and IPP 11 in the Privacy Act as well as information about the likely impact of the introduction of APP 6.[1]

How does the Privacy Act currently regulate use and disclosure?

Use and disclosure

Agencies

IPP 10.1 limits how an agency may use personal information. It starts with the presumption that personal information may only be used for the particular purpose for which it was obtained. This principle is based on the reasonable expectation of the individual concerned that their personal information will only be used by an agency for the purpose for which it was provided. IPP 10.1 (a)–(e) set out 5 exceptions that allow an agency to use personal information for purposes other than that for which it was obtained.

IPP 11.1 limits how an agency may disclose personal information. It provides that personal information must not be disclosed to another person, body or agency other than the individual concerned unless one of the 5 exceptions in IPP 11.1(a)–(e) apply. This principle is based on the concept of confidentiality of client or customer information.

Organisations

National Privacy Principle (NPP) 2 limits how an organisation may use or disclose personal information other than for the primary purpose of collection. Under the exceptions in NPP 2.1(a)–(i), it is not always necessary for an organisation to obtain an individual's consent to use or disclose personal information.

Exceptions

Under IPP 10 and IPP 11 the exceptions concerning use and disclosure of personal information by agencies are broadly the same and include:

— where a person consents

1 IPP 8 and IPP 9 also regulate the use of personal information. They will be replaced by APP 10 – 'quality of personal information'. This will be the subject of a separate fact sheet.

— where the use or disclosure is necessary to protect against a serious and imminent threat to a person's life or health
— where disclosure is:
  – required or authorised by or under law
  – reasonably necessary to enforce the criminal law or a law imposing a pecuniary penalty or to protect public revenue.

Further, a use does not breach IPP 10.1 if the use is directly related to the purpose of collection. A disclosure will not breach IPP 11.1 if the person is reasonably likely to have been aware or has been made aware that information of that kind is usually passed to that person, body or agency.

Recommendations for reform

In its 2008 privacy report *For your information: Australian privacy law and practice*, the Australian Law Reform Commission (ALRC) recommended unification of use and disclosure into a single privacy principle applicable to both agencies and organisations.

The ALRC submitted that unification would reduce the complexity of privacy regulation as well as avoid technical legal arguments about whether an action constitutes a use or disclosure, reducing confusion about which principle should apply.[2]

This recommendation was accepted by the Australian Government in its first stage response to the ALRC's privacy report[3] and will be implemented by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Reform Act).

New APP 6 – use and disclosure of personal information

From 12 March 2014, the principles reflected in IPP 10, IPP 11 and NPP 2 will be unified into new APP 6, which will govern both use and disclosure of personal information by agencies and organisations (collectively known as APP entities).

APP 6.1 provides that, if an APP entity holds personal information that was collected for a particular purpose (the primary purpose), the entity must not use or disclose it for another purpose (the secondary purpose) unless:

— the individual gives consent to the use or disclosure
— the use or disclosure falls within the exceptions set out in APP 6.2 or APP 6.3 of the Reform Act.

Essentially, this APP authorises use and disclosure of personal information for the primary purpose for which it was collected without further consideration. How broadly a 'primary purpose' can be defined will depend on the circumstances of a particular case and is likely to be further developed by the Office of the Australian Information Commissioner (OAIC).[4] However, where agencies wish to use or disclose information for a secondary purpose, they must seek consent or determine whether another exception applies.

Exceptions

Under APP 6.2, use or disclosure of personal information will be authorised where:

— the individual would reasonably expect the APP entity to use or disclose information for the secondary purpose and the secondary purpose is:

2 Australian Law Reform Commission Report 108, *For your information: Australian privacy law and practice*, August 2008, p 843.

3 Australian Government, *Enhancing national privacy protection: Australian Government first stage response to the Australian Law Reform Commission Report 108*, October 2009, p 52.

4 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, Explanatory Memorandum (EM), p 79.

  - directly related to the primary purpose of collection (for sensitive information such as information about an individual's racial or ethnic origin, sexual orientation or criminal record)
  - related to the primary purpose of collection (for non-sensitive information)
- it is required or authorised by or under an Australian law (now defined to include the common law) or a court/tribunal order
- a permitted general situation exists
- a permitted health situation exists
- the APP entity reasonably believes that the use or disclosure is reasonably necessary for enforcement related activities conducted by, or on behalf of, an enforcement body.

Under APP 6.3, disclosure of personal information will be authorised where an agency that is not an enforcement body discloses biometric information or biometric templates to an enforcement body in accordance with guidelines made by the Information Commissioner for the purposes of this exception.

Permitted general situation

'Permitted general situation' is a new concept set out in s 16A of the Reform Act, which provides that a breach of privacy will not occur in relation to the collection, use or disclosure by an APP entity of personal information if the conditions set out in the applicable item in the statutory table in s 16A are met.

Prevention of serious threat to life, health or safety

Permitted general situation 1 will enable an APP entity to collect, use or disclose personal information where it is unreasonable or impractical to obtain consent and the entity reasonably believes that collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety. This exception removes the previous requirement under IPP 10.1(b) and IPP 11.1(c) that a threat be imminent and extends the exception to cover threats to public health and safety.[5] Situations where it may be unreasonable or impractical to obtain consent may include where there is an element of urgency or where the individual's location is unknown.[6]

Unlawful activity

Permitted general situation 2 is a new exception for agencies and will enable an APP entity to collect, use or disclose personal information where the entity:

- has reason to suspect unlawful activity or misconduct of a serious nature that relates to the entity's functions and
- reasonably believes that collection, use or disclosure is necessary in order for the entity to take appropriate action.

This exception may apply in relation to internal agency investigations into fraud or breach of the Australian Public Service Code of Conduct.[7]

Missing persons

Permitted general situation 3 is a new exception for agencies and will enable an APP entity to collect, use or disclose personal information where the entity reasonably believes that it is reasonably

5 Office of the Australian Information Commissioner, *Australian Privacy Principles and Information Privacy Principles – comparison guide*, April 2013, p 21.

6 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, EM, p 67.

7 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, EM, p 67.

necessary to assist any APP entity, body or person to locate a person who has been reported as missing and the collection, use or disclosure complies with rules made by the Information Commissioner.

Legal or equitable claim
Permitted general situation 4 is a new exception for agencies and will enable an APP entity to collect, use or disclose personal information where it is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim. This exception may apply where, for example, an insurance company is gathering information from an agency in order to dispute an insurance claim.[8]

Alternative dispute resolution
Permitted general situation 5 is a new exception for agencies and will enable an APP entity to collect, use or disclose personal information where it is reasonably necessary for the purposes of a confidential alternative dispute resolution process.

Diplomatic or consular functions
Permitted general situation 6 is a new exception that applies only to agencies and will enable an agency to collect, use or disclose personal information where that agency believes that the collection, use or disclosure is necessary for its diplomatic or consular functions or activities.

Defence
Permitted general situation 7 is a new exception for the Defence Force and will enable the Defence Force to collect, use or disclose personal information where it reasonably believes that it is necessary for:

— war or warlike operations
— peacekeeping or peace enforcement
— civil aid
— humanitarian assistance
— medical or civil emergency or disaster relief occurring outside of Australia.

Permitted health situation

'Permitted health situation' is a new concept set out in s 16B of the Reform Act which outlines 5 situations where the collection, use or disclosure of certain health information or genetic information will not be a breach of privacy. These situations reflect exceptions currently contained in the NPPs. It is unlikely that this exception will impact on an agency's activities, as it applies where an organisation (rather than an agency) is collecting, using or disclosing health or genetic information.

Law enforcement

APP 6.2(e) will enable the use or disclosure of personal information if an APP entity reasonably believes that it is reasonably necessary for an enforcement-related activity conducted by, or on behalf of, an enforcement body. 'Enforcement related activities' is a newly defined concept intended to reflect the range of enforcement activities conducted by agencies and includes surveillance activities, intelligence-gathering activities and other monitoring activities as well as protective or custodial activities. For further information see AGS Fact Sheet No 27: *Privacy Act reforms – implications for enforcement functions*.

8 Privacy Amendment (Enhancing Privacy Protection) Bill 2012, EM, p 68.

APP 6.2(e) replaces IPPs 10.1(d) and 11.1(e), relating to 'the enforcement of a criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue'. On its face, APP 6.2(e) is more limited in its application because of the need for the enforcement-related activity to be carried on by, or on behalf of, an enforcement body. Permitted general situation 2 (unlawful activity) may cover some of the same ground for agencies that are not enforcement bodies.

Derivative obligations

Under IPP 11.3, there is an obligation on recipients of personal information disclosed by agencies to use or disclose that information only for the same purpose for which it was disclosed to them. While there is no equivalent obligation contained in the APPs, if the recipient is an APP entity they are bound to deal with the personal information in accordance with the APPs.[9]

How we can assist

While the amendments to the Privacy Act do not commence until 12 March 2014, agencies should act now to ensure they will be ready to meet their new obligations under the Reform Act. AGS has a team of experienced privacy lawyers who can provide more detailed guidance on what the Reform Act will mean for your agency. We are offering training on the changes to the Privacy Act[10] and can also provide practical, focused legal advice to assist your agency in preparing for the reforms.

9 Office of the Australian Information Commissioner, *Australian Privacy Principles and Information Privacy Principles – comparison guide*, April 2013, p 22.

10 See http://www.ags.gov.au/training/index.html

More information please contact

Elena Arduca Senior Executive Lawyer
T 03 9242 1473
elena.arduca@ags.gov.au MELBOURNE

Jane Lye Senior Executive Lawyer
T 07 3360 5736
jane.lye@ags.gov.au BRISBANE

Justin Davidson Senior Executive Lawyer
T 02 6253 7240
justin.davidson@ags.gov.au CANBERRA

Tara McNeilly Senior General Counsel
T 02 6253 7374
tara.mcneilly@ags.gov.au CANBERRA