fact sheet

May 2013

NUMBER 27

Privacy Act reforms – implications for enforcement functions

This fact sheet provides an overview of the current application of the *Privacy Act 1988* to enforcement activities and functions and information about the impact of the reforms to enforcement activities and functions brought about by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (the Reform Act).

How does the Privacy Act currently regulate enforcement functions and activities?

The Privacy Act currently contains 11 Information Privacy Principles (IPPs) which apply to Commonwealth and ACT agencies in their handling of 'personal information' (defined in s 6 of the Privacy Act). The IPPs regulate the collection, storage, use and disclosure of personal information contained in records in the possession or control of an agency.[1]

Most agencies with law enforcement functions already are covered by the Privacy Act, with the exception of the Australian Crime Commission (ACC) and the Integrity Commissioner and staff members of the Australian Commission for Law Enforcement Integrity (ACLEI).

A number of exceptions for enforcement activities also currently exist in the IPPs. For example, IPP 10 provides that an agency must not use personal information for a purpose other than the particular purpose for which it was obtained, except in any of the circumstances specified in that IPP. Similarly, IPP 11 provides that an agency must not disclose personal information except in any of the circumstances specified in IPP 11. The excepted circumstances listed in IPPs 10 and 11 include where a use or disclosure is reasonably necessary for 'the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue'.[2]

Amendments to the Privacy Act for enforcement activities

The Reform Act puts into practice the Government's first-stage response to the Australian Law Reform Commission (ALRC) report, *For your information: Australian privacy law and practice*. The Reform Act passed through Parliament on 29 November 2012 and received royal assent on 12 December 2012. The reforms discussed in this fact sheet are to commence on 12 March 2014.

The Reform Act will repeal the IPPs and the National Privacy Principles (NPPs) (which apply to the private sector). These will be replaced by the Australian Privacy Principles (APPs) – a single set of privacy principles applying to both Commonwealth agencies and private sector organisations (which are referred to as 'APP entities').

1 A 'use' of information generally relates to managing personal information within an agency, whereas a 'disclosure' is interpreted as a release of personal information from the effective control of the agency (see the Privacy Commissioner's *Plain English Guidelines to Information Privacy Principles 8–11*, November 1996, available at www.privacy.gov.au).

2 See IPP 10.1(d) and IPP 11.1(e). Enforcement bodies may also be governed by laws that purport to set out the categories of all permitted uses and disclosure and can rely on the exceptions in the IPPs that allow a use or disclosure where it is required or authorised by or under law (see IPP 10.1(c) and IPP 11.1(d)).

Definitions

Under the Reform Act, the definition of an 'enforcement body' in s 6(1) of the Privacy Act will be expanded to include CrimTrac, the Immigration Department (defined by the Reform Act to mean the Department 'administered by the Minister administering the *Migration Act 1958*') and the Office of the Director of Public Prosecutions (DPP) or a similar body established under a law of a State or Territory.[3] The pre-existing bodies listed in s 6(1) have been retained.[4]

A definition of 'enforcement-related activity' is also introduced into s 6(1) of the Privacy Act by the Reform Act. 'Enforcement-related activity' is to include the prevention, detection, investigation, prosecution and punishment of criminal offences, as well as the breach of a law imposing a penalty or sanction. It also includes surveillance activities, intelligence gathering or monitoring, protecting the public revenue and preparation for, or conduct of, proceedings before a court or tribunal.

These definitions in s 6(1) will be important when applying the new set of APPs introduced by the Reform Act because the APPs create certain exceptions that are relevant to 'enforcement bodies' or 'enforcement-related activity'.

Sensitive information

New APP 3 relates to the collection of personal information and makes a distinction between the collection of personal information and the collection of sensitive information.[5]

APP 3.3 makes it clear that sensitive information can only be collected by APP entities in restricted circumstances: where either the individual consents to the collection and there is a relevant link to the entity's functions and activities or one of the exceptions in APP 3.4 applies. Significantly, the exception in APP 3.4(d) provides that an enforcement body can collect sensitive information if it reasonably believes the collection is reasonably necessary for, or directly related to, 1 or more of its functions or activities. This rule is slightly modified for the Immigration Department, as discussed further below.

The Explanatory Memorandum (EM) to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Privacy Amendment Bill) notes:

> ... this exception enables agencies with law enforcement functions and activities to be able to collect sensitive information without consent to perform their lawful and legitimate functions and activities. There is a strong public interest in enabling law enforcement agencies to enforce the criminal law. A major part of this important function is the ability to collect information about individuals. An additional safeguard is that these agencies are also subject to significant accountability and oversight arrangements over their activities.[6]

The exception in APP 3.4(d) means that an enforcement body may collect sensitive information without the consent of the individual concerned if the collection is necessary or directly related to their ability to perform their lawful and legitimate functions and activities. For example, it may apply in circumstances where the collection of sensitive information directly from the individual concerned is not possible or would be likely to prejudice an investigation.

---

3 The Explanatory Memorandum (EM) to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (the Privacy Amendment Bill) notes that a body will be similar to the Office of the Director of Public Prosecutions (DPP) if it has similar enforcement-related functions. The EM notes that DPP offices may, to some extent, already come within paragraphs (f) and (g) of the existing definition of enforcement body in s 6 but to avoid any doubt they have been included in the amended definition.

4 These include the Australian Federal Police, the Australian Crime Commission, Customs, the Australian Prudential Regulation Authority, the Australian Securities and Investments Commission and various State or Territory law enforcement agencies and other agencies or bodies to the extent they are 'responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law' or responsible for administering a law relating to the protection of the public revenue'.

5 Sensitive personal information includes information or opinion about an individual's racial or ethnic origin, political opinions and association, religious beliefs or affiliations, philosophical beliefs, sexual preferences or practices, trade or professional associations and memberships, union membership, criminal record, and health or genetic information. From 12 March 2014 it will also include biometric information.

6 See Privacy Amendment Bill, EM, p 76.

The application of the exception in APP 3.4(d) depends upon whether the enforcement body has a 'reasonable belief' that the collection is 'reasonably necessary'. According to the EM to the Privacy Amendment Bill, the 'reasonable belief test' will allow entities to make decisions based on 'the information available to them and the context of a particular disclosure'. The phrase 'reasonably necessary' has generally not required that an action be essential or critical but must be something more than 'just helpful, or of some assistance, or expedient'.[7]

In the case of the Immigration Department, APP 3.4(d)(i) provides that the collection of sensitive information is only permitted where it is 'reasonably necessary for, or directly related to, 1 or more enforcement activities conducted by, or on behalf of, the entity'. It is clear from the EM to the Privacy Amendment Bill that this distinction between the Immigration Department and other enforcement bodies is included because of the range of non-enforcement functions and activities undertaken by the Immigration Department and the need to limit the collection of sensitive information to enforcement-related activities.

Use and disclosure

New APP 6 provides that, if an APP entity holds personal information about an individual that was collected for a particular purpose, the entity must not use or disclose the information for another purpose unless either:

— the individual has consented to the use or disclosure

— one of the exceptions in APP 6.2 or APP 6.3 applies.

The exception in APP 6.2(e) provides that an APP entity can use or disclose personal information if it reasonably believes that the use or disclosure is reasonably necessary for 1 or more enforcement-related activities conducted by, or on behalf of, an enforcement body. The EM indicates this exception is 'aimed at enabling any APP entity to cooperate with an enforcement body where it may have personal information relevant to an enforcement related activity of that enforcement body'. However, it is a requirement in APP 6.5 that an APP entity must make a written note of any use or disclosure in accordance with the exception in APP 6.2(e). The purpose of APP 6.5 is to ensure that APP entities remain accountable for such disclosures.[8]

Cross-border disclosure – overseas recipients

APP 8 sets out a requirement for an APP entity that chooses to disclose personal information to overseas recipients to take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs.

The 'requirement to take such steps as are reasonable in the circumstances' is qualified by a number of exceptions, including APP 8.2(e), which permits a disclosure by an agency where it is 'required or authorised by or under an international agreement relating to information sharing to which Australia is a party'. The EM to the Privacy Amendment Bill makes it clear that this exception is intended to include all forms of information-sharing agreements made between Australian agencies and international counterparts and could include a treaty or exchange of letters. The effect of APP 8.2(e) is that an enforcement body would not have to take steps before disclosing personal information to an overseas recipient if the disclosure was made in connection with one of Australia's international information-sharing agreements, such as a double taxation agreement.

7 For example, see the Privacy Commissioner's *Plain English Guidelines to Information Privacy Principles 8–11*, November 1996, p 47, available at www.privacy.gov.au

8 Privacy Amendment Bill, EM, p 80.

The exception in APP 8.2(f) may also be available where an agency reasonably believes that a disclosure is reasonably necessary for enforcement-related activities conducted by, or on behalf of, an enforcement body and the recipient is a body that performs functions or exercises powers that are similar to those performed or exercised by an enforcement body. The EM makes it clear that this exception 'is intended to enable an enforcement body to cooperate with international counterparts for enforcement related activities without having to take steps to ensure compliance with the APPs'.[9]

Government identifiers

The Reform Act defines a 'government-related identifier' as an identifier of an individual that has been assigned by an agency, a State or Territory authority or an agent or contracted service provider of an agency or State or Territory authority.

New APP 9 regulates the adoption, use or disclosure of government-related identifiers by organisations. It aims to restrict the use of government-related identifiers by the private sector so that government-related identifiers do not become universal identifiers.

APP 9.2 provides certain exceptions relating to the use and disclosure of government-related identifiers. In particular, APP 9.2(e) allows for a use or disclosure of a government-related identifier where an organisation reasonably believes it is reasonably necessary for enforcement-related activities conducted by, or on behalf of, an enforcement body. The EM to the Privacy Amendment Bill indicates that the use of 'reasonably necessary' in this exception ensures that an objective test is applied.

9 Privacy Amendment Bill, EM, p 84.

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