Chapter 8:

Australian Privacy Principle 8 —

Cross-border disclosure of personal information

Version 1.2, July 2019

OAIC

Contents

Key points

- Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information (APP 8.1).
- An APP entity that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient in relation to the information that would breach the APPs (s 16C).
- There are exceptions to the requirement in APP 8.1 to take reasonable steps and to the accountability provision in s 16C.

What does APP 8 say?

8.1 APP 8 and s 16C create a framework for the cross-border disclosure of personal information. The framework generally requires an APP entity to ensure that an overseas recipient will handle an individual's personal information in accordance with the APPs, and makes the APP entity accountable if the overseas recipient mishandles the information.[1] This reflects a central object of the Privacy Act, of facilitating the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f)).

8.2 APP 8.1 provides that before an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C).

8.3 There are exceptions to the requirement in APP 8.1 and to the accountability provision in s 16C (see paragraphs 8.19–8.55 below).

8.4 When an APP entity discloses personal information to an overseas recipient it will also need to comply with APP 6. That is, it must only disclose the personal information for the primary purpose for which it was collected unless an exception to that principle applies (see Chapter 6 (APP 6)). A note to APP 6.1 cross-references the requirements for the cross-border disclosure of personal information in APP 8. It is implicit in this note, that APP 8 only applies to personal information covered by APP 6. That is, it only applies to personal information 'held' by an APP entity. The term 'holds' is discussed in Chapter B (Key concepts).

'Overseas recipient'

8.5 Under APP 8.1, an 'overseas recipient' is a person who receives personal information from an APP entity and is:

- not in Australia or an external Territory

[1] An accountability approach was adopted in the Asia-Pacific Economic Cooperation (APEC) Privacy Framework in 2004, Information Privacy Principle IX (Accountability), see APEC website <publications.apec.org>. The accountability concept in the APEC Privacy Framework was in turn derived from the accountability principle from the Organisation for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 1980, see OECD website <https://www.oecd.org>.

- not the APP entity disclosing the personal information, and
- not the individual to whom the personal information relates

8.6 This means that where an APP entity in Australia sends information to an overseas office of the entity, APP 8 will not apply as the recipient is the same entity.[2] This is to be distinguished from the case where an APP entity in Australia sends personal information to a 'related body corporate' located outside of Australia.[3] In that case, the related body corporate is a different entity to the APP entity in Australia. It will therefore be an 'overseas recipient' and APP 8 will apply.[4]

When does an APP entity 'disclose' personal information about an individual to an overseas recipient?

8.7 The term 'disclose' is not defined in the Privacy Act.

8.8 An APP entity discloses personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. The release of the information may be a proactive release or publication, a release in response to a specific request, an accidental release or an unauthorised release by an employee.[5] This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure. Further, there will be a disclosure in these circumstances even where the information is already known to the overseas recipient.

8.9 In the context of APP 8, an APP entity will disclose personal information to an overseas recipient where it, for example:

- shares the personal information with an overseas recipient
- reveals the personal information at an international conference or meeting overseas
- sends a hard copy document or email containing an individual's personal information to an overseas client
- publishes the personal information on the internet, whether intentionally or not, and it is accessible to an overseas recipient.

8.10 'Disclosure' is a separate concept from:

- 'unauthorised access' which is addressed in APP 11. An APP entity is not taken to have disclosed personal information where a third party intentionally exploits the entity's

[2] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

[3] Section 6(8) provides 'for the purposes of this Act, the question whether bodies corporate are related to each other is determined in the manner in which that question is determined under the Corporations Act 2001.'

[4] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 states 'APP 8 will apply where an organisation sends personal information to a 'related body corporate' located outside Australia' (p 83). While s 13B(1) permits related bodies corporate to share personal information (unless an exception applies), it does not exempt an APP entity from complying with APP 8 before it discloses personal information to a related body corporate located overseas.

[5] An APP entity is taken to have 'disclosed' personal information where an employee carries out an unauthorised disclosure 'in the performance of the duties of the person's employment' (s 8(1)).

security measures and gains unauthorised access to the personal information. Examples include unauthorised access following a cyber-attack[6] or a theft, including where the third party then makes that personal information available to others outside the entity.[7] However, where a third party gains unauthorised access, the APP entity may breach APP 11 if it did not take reasonable steps to protect the personal information from unauthorised access (see Chapter 11 (APP 11))

- 'use'. An APP entity uses personal information where it handles, or undertakes an activity with the personal information, within the entity's effective control. For example, where an entity provides personal information to an overseas recipient, via a server in a different overseas location, there would not usually be a disclosure until the personal information reaches the overseas recipient. That is, routing personal information, in transit, through servers located outside Australia, would usually be considered a 'use'.[8] In limited circumstances, the provision of personal information to a contractor may also be a 'use' of that personal information (see paragraphs 8.12–8.15 below).

8.11 For further information about the concepts of 'use' and 'disclosure' of personal information, see Chapter B (Key concepts).

Providing personal information to a contractor

8.12 Where an APP entity engages a contractor located overseas to perform services on its behalf, in most circumstances, the provision of personal information to that contractor is a disclosure. This means that the entity will need to comply with APP 8 before making that disclosure. Where a subcontractor may be engaged, the entity should also take reasonable steps to ensure that the subcontractor does not breach the APPs in relation to the personal information.[9]

8.13 For example, the provision of personal information to a contractor is generally considered a 'disclosure' where:

- an Australian based retailer outsources the processing of online purchases through its website to an overseas contractor and, in order to facilitate this, provides the overseas contractor with personal information about its customers
- an Australian entity, as part of a recruitment drive, provides the personal information of job applicants to an overseas services provider to perform reference checks on behalf of the Australian entity
- an Australian organisation relies on its overseas parent company to provide technical and billing support, and as part of this, provides the overseas parent company with access to its Australian customer database (which includes personal information)

8.14 However, in limited circumstances providing personal information to an overseas contractor to perform services on behalf of the APP entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control. In these circumstances, the entity would not need to comply with

---

[6] See OAIC, Sony PlayStation Network / Qriocity: Own Motion Investigation Report, September 2011, OAIC website <https://www.oaic.gov.au>.

[7] The actions of an employee will be attributed to the APP entity where it was carried out 'in the performance of the duties of the person's employment' (s 8(1)).

[8] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

[9] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

APP 8. For example, where an APP entity provides personal information to a cloud service provider located overseas for the limited purpose of performing the services of storing and ensuring the entity may access the personal information, this may be a 'use' by the entity in the following circumstances:

- a binding contract between the entity and the provider requires the provider only to handle the personal information for these limited purposes
- the contract requires any subcontractors to agree to the same obligations, and
- the contract gives the entity effective control of how the personal information is handled by the overseas recipient. Issues to consider include whether the entity retains the right or power to access, change or retrieve the personal information, who else will be able to access the personal information and for what purposes, what type of security measures will be used for the storage and management of the personal information (see also APP 11.1, Chapter 11) and whether the personal information can be retrieved or permanently deleted by the entity when no longer required or at the end of the contract.[10]

8.15 Where the provision of personal information to an overseas contractor is a use, an APP entity may breach the APPs if the information is mishandled while in the overseas contractor's physical possession. This is because the APP entity is considered to still 'hold' the information (as it has effective control of the information), and a number of APPs apply to an entity that 'holds' personal information ('holds' is discussed in Chapter B (Key Concepts)).

Taking reasonable steps to ensure an overseas recipient does not breach the APPs

8.16 The requirement in APP 8.1 to ensure that an overseas recipient does not breach the APPs is qualified by a 'reasonable steps' test. It is generally expected that an APP entity will enter into an enforceable contractual arrangement with the overseas recipient that requires the recipient to handle the personal information in accordance with the APPs (other than APP 1).[11] Contractual arrangements may include:

- the types of personal information to be disclosed and the purpose of disclosure
- a requirement that the overseas recipient complies with the APPs in relation to the collection, use, disclosure, storage and destruction or de-identification of personal information. This should also require the overseas recipient to enter a similar contractual arrangement with any third parties to whom it discloses the personal information (for example, a subcontractor)
- the complaint handling process for privacy complaints
- a requirement that the recipient implement a data breach response plan which includes a mechanism for notifying the APP entity where there are reasonable grounds to suspect

[10] For further discussion of cloud computing considerations for agencies, see Secure Cloud Strategy, Digital Transformation Agency website <https://www.dta.gov.au>.

[11] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

a data breach and outlines appropriate remedial action (based on the type of personal information to be handled under the contract)[12]

8.17 However, whether reasonable steps to ensure the overseas recipient does not breach the APPs requires a contract to be entered into, the terms of the contract, and the steps the APP entity takes to monitor compliance with any contract (such as auditing), will depend upon the circumstances that include:

- the sensitivity of the personal information. More rigorous steps may be required if the information is 'sensitive information' (defined in s 6(1) and discussed in Chapter B (Key concepts)) or other personal information of a sensitive nature
- the entity's relationship with the overseas recipient. More rigorous steps may be required if an entity discloses information to an overseas recipient to which it has not previously disclosed personal information
- the possible adverse consequences for an individual if the information is mishandled by the overseas recipient. More rigorous steps may be required as the risk of adversity increases.
- existing technical and operational safeguards implemented by the overseas recipient which will protect the privacy of the personal information — more rigorous steps may be required where the recipient has limited safeguards in place
- the practicability, including time and cost involved. However, an entity is not excused from ensuring that an overseas recipient does not breach the APPs by reason only that it would be inconvenient, time-consuming or impose some cost to do so. Whether these factors make it unreasonable to take particular steps will depend on whether the burden is excessive in all the circumstances.

8.18 Where an agency discloses personal information to a recipient that is engaged as a contracted service provider, the agency must also comply with s 95B. Section 95B(1) provides that an agency must take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice, that would breach an APP if done by that agency. The contract must contain provisions to ensure that such an act or practice is not authorised by a subcontract (s 95B(3)). Contractual measures taken under s 95B will generally satisfy the requirement in APP 8.1.

Disclosing personal information to an overseas recipient that is subject to a substantially similar law or binding scheme

8.19 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity reasonably believes that:

- the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way the APPs protect the information, and

[12] See OAIC, Data Breach Preparation and Response, OAIC website <https://www.oaic.gov.au>.

- mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme (APP 8.2(a))

Reasonable belief

8.20 The term 'reasonably believe' is discussed in Chapter B (Key concepts). In summary, an APP entity must have a reasonable basis for its belief, and not merely a genuine or subjective belief. For example, this might be based on independent legal advice. It is the responsibility of an APP entity to be able to justify its reasonable belief.

Law or binding scheme

8.21 An overseas recipient may be subject to a law or binding scheme, where, for example, it is:

- bound by a privacy or data protection law that applies in the jurisdiction of the recipient
- required to comply with another law that imposes obligations in relation to the handling of personal information, for example some taxation law includes provisions that expressly authorise and prohibit specified uses and disclosures, permit the retention of some data, require destruction after a certain period of time and under particular circumstances, and include a right of access to an individual's personal information
- subject to an industry scheme or privacy code that is enforceable once entered into, irrespective of whether the recipient was obliged or volunteered to participate or subscribe to the scheme or code
- subject to Binding Corporate Rules (BCRs). BCRs allow multinational corporations, international organisations and groups of companies to make intra-organisational transfers of personal information across borders in compliance with EU Data Protection law.[13] BCRs typically form a stringent, intra-corporate global privacy policy that satisfies EU standards. The Article 29 Working Party issued several guidance documents on BCR content, acceptance criteria and submission process.[14]

8.22 However, an overseas recipient may not be subject to a law or binding scheme where, for example:

- the overseas recipient is exempt from complying, or is authorised not to comply, with part, or all of the privacy or data protection law in the jurisdiction
- the recipient can opt out of the binding scheme without notice and without returning or destroying the personal information

Substantially similar to

8.23 A substantially similar law or binding scheme would provide a comparable, or a higher level of privacy protection to that provided by the APPs. Each provision of the law or scheme is not required to correspond directly to an equivalent APP. Rather, the overall effect of the law or scheme is of central importance.

[13] European Commission website <https://ec.europa.eu/info/law/law-topic/data-protection_en>.

[14] Available at European Commission website <https://ec.europa.eu/info/law/law-topic/data-protection_en>. See in particular documents WP 133 (2007), WP 153 (2008), WP 154 (2008), WP 155 (2008).

8.24 Whether there is substantial similarity is a question of fact. Factors that may indicate that the overall effect is substantially similar, include:

- the law or scheme includes a comparable definition of personal information that would apply to the personal information disclosed to the recipient
- the law or scheme regulates the collection of personal information in a comparable way
- the law or scheme requires the recipient to notify individuals about the collection of their personal information
- the law or scheme requires the recipient to only use or disclose the personal information for authorised purposes
- the law or scheme includes comparable data quality and data security standards
- the law or scheme includes a right to access and seek correction of personal information

Mechanisms to enforce privacy protections

8.25 An enforcement mechanism should meet two key requirements: it should be accessible to the individual and it should have effective powers to enforce the privacy or data protections in the law or binding scheme. A range of mechanisms may satisfy those requirements, ranging from a regulatory body similar to the Office of the Australian Information Commissioner (the OAIC), to an accredited dispute resolution scheme, an independent tribunal or a court with judicial functions and powers. Factors that may be relevant in deciding whether there is an accessible and effective enforcement mechanism include whether the mechanism:

- is independent of the overseas recipient that is required by the law or binding scheme to comply with the privacy or data protections
- has authority to consider a breach of any of the privacy or data protections in the law or binding scheme
- is accessible to an individual, for example, the existence of the scheme is publicly known, and can be accessed by individuals directly and without payment of any unreasonable charge
- has the power to make a finding that the overseas recipient is in breach of the law or binding scheme and to provide a remedy to the individual
- is required to operate according to principles of procedural fairness

8.26 The mechanism may be a single mechanism or a combination of mechanisms. It may be established by the law or binding scheme that contains the privacy or data protections, or by another law or binding scheme. Alternatively, the mechanism may take effect through the operation of cross-border enforcement arrangements between the OAIC and an appropriate regulatory authority in the foreign jurisdiction.[15]

[15] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 83.

Disclosing personal information to an overseas recipient with the individual's consent after the individual is expressly informed

8.27 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the APP entity expressly informs the individual that if they consent to the disclosure, this principle will not apply, and
- the individual then consents to the disclosure (APP 8.2(b))

Expressly inform

8.28 An APP entity should provide the individual with a clear written or oral statement explaining the potential consequences of providing consent. At a minimum, this statement should explain that if the individual consents to the disclosure and the overseas recipient handles the personal information in breach of the APPs:

- the entity will not be accountable under the Privacy Act
- the individual will not be able to seek redress under the Privacy Act

8.29 The statement should also:

- be made at the time consent is sought
- not rely on assumed prior knowledge of the individual

8.30 The statement could also explain any other practical effects or risks associated with the disclosure that the APP entity is aware of, or would be reasonably expected to be aware of. These may include that:

- the overseas recipient may not be subject to any privacy obligations or to any principles similar to the APPs
- the individual may not be able to seek redress in the overseas jurisdiction
- the overseas recipient is subject to a foreign law that could compel the disclosure of personal information to a third party, such as an overseas authority

Consent

8.31 Consent is defined in s 6(1) as 'express consent or implied consent', and is discussed in more detail in Chapter B (Key concepts). The four key elements of consent are:

- the individual is adequately informed before giving consent (in this case 'expressly informed')
- the individual gives consent voluntarily
- the consent is current and specific, and
- the individual has the capacity to understand and communicate their consent

8.32 An APP entity does not need to obtain consent before every proposed cross-border disclosure.[16] It may obtain an individual's consent to disclose a particular kind of personal information to the same overseas recipient for the same purpose on multiple occasions, providing it has expressly informed the individual of the potential consequences of providing that consent. In doing this, the entity should not seek a broader consent than is necessary for its purposes, for example, consent for undefined future uses, or consent to all legitimate uses or disclosures.

8.33 If an individual withdraws their consent, the APP entity must no longer rely on the original consent when dealing with the individual's personal information.

Disclosing personal information to an overseas recipient as required or authorised by law

8.34 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is 'required or authorised by or under an Australian law or a court/tribunal order' (APP 8.2(c)). An APP entity cannot rely on a requirement or authorisation in an overseas jurisdiction (see paragraphs 8.60–8.64 below). The meaning of 'required or authorised by or under an Australian law or a court/tribunal order' is discussed in Chapter B (Key concepts).

8.35 The following are examples of where a law or order may require or authorise disclosure of personal information to an overseas recipient:

- an APP entity disclosing personal information to the government of a foreign country under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)
- an agency disclosing personal information to an overseas recipient under the Australian Federal Police Act 1979 (Cth) or the Mutual Assistance in Criminal Matters Act 1987 (Cth)

8.36 An agency that intends to rely on this exception could consider establishing administrative arrangements, memorandums of understanding or protocols with the overseas recipient that set out mutually agreed standards for the handling of personal information that provide privacy protections comparable to the APPs (see discussion of contractual measures in paragraphs 8.16–8.18 above).

Disclosing personal information to an overseas recipient where a permitted general situation exists

8.37 The cross-border principle will not apply if a permitted general situation exists for that disclosure (APP 8.2(d)). Section 16A lists five permitted general situations that may exist for a cross border disclosure. These situations are set out below, and are discussed in more detail in Chapter C (Permitted general situations) (including the meaning of relevant terms).

[16] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.

Lessening or preventing a serious threat to life, health or safety

8.38 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- it is unreasonable or impracticable to obtain the individual's consent to the disclosure, and
- the entity reasonably believes the 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 (s 16A(1), Item 1)

8.39 For example, this permitted general situation might apply where an APP entity discloses the personal information of an individual to a foreign authority, based on a reasonable belief that this disclosure will lessen a serious threat to the health or safety of that individual's children, but seeking the individual's consent may increase the threat.

Taking appropriate action in relation to suspected unlawful activity or serious misconduct

8.40 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where the entity:

- has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in, and
- reasonably believes that the cross-border disclosure is necessary for the entity to take appropriate action in relation to the matter (s 16A(1), Item 2)

8.41 For example, this permitted general situation may apply where an APP entity that is a global organisation has reason to suspect that an individual is engaging in transnational fraud affecting the entity's activities, and the entity reasonably believes that disclosing personal information to an overseas authority is necessary to take appropriate action.

Locating a person reported as missing

8.42 An APP entity may disclose personal information to an overseas recipient without complying with APP 8.1 where:

- the entity reasonably believes that the disclosure is reasonably necessary to assist any APP entity, body or person to locate a person who has been reported as missing, and
- the disclosure complies with rules made by the Information Commissioner under s 16A(2) (s 16A(1), Item 3)

Necessary for a diplomatic or consular function or activity

8.43 An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where the agency reasonably believes that the disclosure is necessary for the agency's diplomatic or consular functions or activities (s 16A(1), Item 6). The permitted general situation applies only to agencies, and not to organisations.

8.44 For example, this permitted general situation may apply where an agency discloses personal information to an overseas recipient to assist an Australian citizen who is in distress overseas, such as where an Australian individual is detained or is the victim of crime, where assistance is required with repatriation in the case of death or serious illness, or to provide assistance in response to a crisis or emergency overseas.

Necessary for certain Defence Force activities outside Australia

8.45 The Defence Force (as defined in s 6(1)) may disclose personal information to an overseas recipient without complying with APP 8.1 where it reasonably believes that the disclosure is necessary for a warlike operation, peacekeeping, civil aid, humanitarian assistance, a medical emergency, a civil emergency or disaster relief occurring outside Australia and the external Territories (s 16A(1), Item 7).

8.46 For example, this permitted general situation might apply where, in the immediate aftermath of a natural or man-made disaster outside Australia, the Defence Force discloses an individual's personal information to an overseas recipient in order to assist in the provision of proper medical care to that individual.

Disclosing personal information to an overseas recipient as required or authorised under an international agreement relating to information sharing

8.47 An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where the disclosure is 'required or authorised by or under an international agreement relating to information sharing to which Australia is a party' (APP 8.2(e)). This exception does not apply to organisations.

8.48 The term 'international agreement' is not defined in the Privacy Act. This guideline clarifies that the term includes documents binding at international law (for example, treaties and conventions), as well as other formal written documents not binding at international law (for example, a memorandum of understanding or an official exchange of letters[17]) that provide for information sharing between an agency and an overseas recipient. This exception applies only to such documents where the parties are Australia and one or more foreign states, although the overseas recipient of shared information may be a non-state entity.

8.49 Information sharing may not be the only or the primary subject of the agreement, so long as the agreement makes provision for 'information sharing'. Additionally, the disclosure of personal information to the overseas recipient must be 'required or authorised' by or under the agreement.

8.50 To meet those requirements, the agreement should make specific arrangements for disclosure of information to an overseas recipient, including identifying the agency and the overseas recipient, the categories of personal information that may be disclosed to the recipient under the agreement and the circumstances in which or the purposes for which the

[17] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84

information will be disclosed. This exception is unlikely to apply to an agreement that contains only a general commitment by the parties to facilitate, or remove obstacles to, the disclosure or exchange of information (the terms 'required' and 'authorised' are discussed in more detail in Chapter B (Key concepts)).

8.51 The agreement could also include provisions dealing with the responsibility of the parties to ensure adequate protection of the personal information that is disclosed according to standards comparable to those in the APPs, and the procedure to be followed to ensure that obligations or undertakings imposed by the agreement are met. The discussion of contractual measures in paragraphs 8.16–8.18 above lists other matters that could be considered for inclusion the agreement.

Disclosing personal information to an overseas recipient for an enforcement related activity

8.52 An agency may disclose personal information to an overseas recipient without complying with APP 8.1 where both of the following apply:

- the agency reasonably believes that the disclosure is reasonably necessary for one or more 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 (APP 8.2(f))

8.53 This exception is intended to enable an agency that is an enforcement body to cooperate with international counterparts for enforcement related activities.

8.54 'Enforcement body' is defined in s 6(1) as a list of specific bodies and is discussed in Chapter B (Key concepts). The list includes Commonwealth, State and Territory bodies that are responsible for policing, criminal investigations, and administering laws to protect the public revenue or to impose penalties or sanctions. Examples of Commonwealth enforcement bodies are the Australian Federal Police, Australian Crime Commission,[18] the Integrity Commissioner,[19] the Immigration Department,[20] Australian Prudential Regulation Authority, Australian Securities and Investments Commission and AUSTRAC.

8.55 'Enforcement related activities' is defined in s 6(1) and discussed in Chapter B (Key concepts). For further discussion of a similar exception in APP 6.2(e), see Chapter 6 (APP 6).

[18] In July 2016, the former Australian Crime Commission and CrimTrac were merged to form the Australian Criminal Intelligence Commission.

[19] 'Integrity Commissioner' is defined in s 6(1) as having the same meaning as in the Law Enforcement Integrity Commissioner Act 2006.

[20] 'Immigration Department' is defined in s 6(1) as the Department administered by the Minister administering the Migration Act 1958. This is now the Department of Home Affairs.

When is an APP entity accountable for personal information that it discloses to an overseas recipient?

8.56 An APP entity that discloses personal information to an overseas recipient is accountable, in certain circumstances, for an act or practice of the overseas recipient in relation to the information that would breach the APPs (s 16C(1)). Accountable means that the act or practice is taken to have been done by the APP entity and to be a breach of the APPs by that entity (s 16C(2)).

8.57 This accountability provision applies where:

- APP 8.1 applies to the disclosure. That is, none of the exceptions in APP 8.2 apply to the disclosure
- the APPs do not apply to the overseas recipient in relation to the personal information (for more information about when the APPs will apply see Chapter A (Introductory matters)), and
- an act or practice by the overseas recipient would breach the APPs (other than APP 1) if they had applied (s 16C(1))

8.58 Under the accountability provision, an APP entity may be liable for the acts or practices of the overseas recipient (and the individual will have a means of redress) even where:

- the entity has taken reasonable steps to ensure the overseas recipient complies with the APPs (see APP 8.1) and the overseas recipient subsequently does an act or practice that would breach the APPs
- the overseas recipient discloses the individual's personal information to a subcontractor and the subcontractor breaches the APPs[21]
- the overseas recipient inadvertently breaches the APPs in relation to the information

8.59 However, an APP entity will not be accountable where, for example, it discloses personal information to an overseas recipient under an exception in APP 8.2 (see paragraphs 8.19–8.55 above), or where personal information is disclosed to an overseas recipient with an 'Australian link'. A recipient that has an 'Australian link' will be covered by the Privacy Act. 'Australian link' is defined in s 5B(2) and discussed in more detail in Chapter B (Key concepts).

Overseas acts or practices required by a foreign law

8.60 Section 6A(4) provides that an act or practice required by an applicable law of a foreign country will not breach the APPs if it is done, or engaged in, outside Australia and the external Territories. The meaning of 'required' by a law is discussed in Chapter B (Key concepts).

8.61 The effect of this provision is that where an overseas recipient of personal information does an act or practice that is required by an applicable foreign law, this will not breach the APPs.

[21] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 84.

The APP entity will also not be responsible for the act or practice under the accountability provision.

8.62 For example, the USA PATRIOT Act may require the overseas recipient to disclose personal information to the Government of the United States of America.[22] In these circumstances, the APP entity would not be responsible under the accountability provision for the disclosure required by that Act.

8.63 An APP entity could consider notifying an individual, if applicable, that the overseas recipient may be required to disclose their personal information under a foreign law. The entity could also explain that the disclosure will not breach the APPs. This information could be included in the APP entity's APP 5 notice, particularly if the entity usually discloses personal information to overseas recipients (see APP 5.2(i), Chapter 5), or in its APP Privacy Policy (see Chapter 1 (APP 1)).

8.64 This provision does not apply to acts or practices that are done or engaged in, within Australia. Where a foreign law requires an APP entity in Australia to disclose personal information to an overseas recipient the entity must comply with APPs 6 and 8.

[22] See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001 (USA).