# Chapter 11

# Australian Privacy Principle 8–cross-border disclosure of personal information and sections 19 and 20

## Introduction

11.1 Australian Privacy Principle 8 (APP 8) outlines measures to ensure that entities cannot avoid obligations to protect personal information by disclosing the information to a recipient outside Australia.[1] Section 19 provides for the extra-territorial operation of the new Privacy Act.[2] Section 20 provides that an entity remains accountable for the acts and practices of overseas recipients to which it discloses personal information.[3]

11.2 The Companion Guide notes that APP 8 uses the term 'disclosure', rather than 'transfer', which was used in National Privacy Principle 9 (NPP 9) as 'transfer' implies that there is a cross-border movement of personal information rather than the accessing of personal information by an overseas recipient, regardless of whether the information is stored in Australia or elsewhere through 'disclosure'. The Companion Guide notes that the routing of personal information through servers which are located outside of Australia is not intended to constitute a disclosure.[4]

11.3 APP 8 has been extended to apply to agencies as well as organisations.[5] In addition, APP 8 provides conditions for the disclosure of personal information outside Australia to ensure that entities remain accountable for any disclosures they make, rather than prohibiting cross-border disclosures all together as is the case under NPP 9. However, a series of exceptions provide for an entity not to be held accountable for the disclosure of personal information to an overseas recipient.[6]

11.4 The principle provides that before disclosing any personal information outside of Australia, an entity has to take 'reasonable steps' to ensure that the overseas recipient will not breach the APPs, by making sure that personal information has sufficient protection. The Companion Guide notes it is expected that the obligations of the overseas recipient would be set out in a contract to establish effective information management arrangements.[7]

---

1 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

2 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 6–7.

3 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

4 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

5 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

6 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

7 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

11.5 Section 19 provides for the extraterritorial operation of the Act. In addition, unlike the *Privacy Act 1988* (Privacy Act) which only extended to the acts or practices undertaken by an organisation outside of Australia in relation to the personal information of Australian citizens or permanent residents, the new Privacy Act will extend to protect every person, operating in relation to acts done or practices engaged in outside of Australia, by agencies and organisations with an Australian link.[8] The definition of an 'Australian link' is similar to that provided under subsection 5B(2) of the current Privacy Act.[9]

11.6 The Companion Guide also states that arrangements under the existing Privacy Act which ensure that an act or practice that is done or engaged in outside Australia is not an interference with privacy if the act or practice is required by an applicable law of a foreign country, will be replicated in the new Privacy Act. These provisions will extend to cover agencies as well as organisations.[10]

11.7 Under proposed section 20, an entity is held accountable for the acts and practices of overseas recipients.[11] The Companion Guide notes that while the term 'accountability' is not used in this section, the provisions of the section hold an entity as liable for the acts and practices of an overseas recipient which breach the APPs. However, if one of the exceptions under APP 8 applies to the entity, then section 20 will not apply to the entity.[12]

## Background

11.8 The transfer of personal information across national borders has been identified as an issue of significant community concern. However, technological advancements, among other developments, have contributed to a change in the way business is conducted, and how personal information is collected and managed.[13] A submitter to the Australian Law Reform Commission (ALRC) review commented:

> In today's truly globalised world, cross-border data flows are an everyday fact of commercial public and private life. The challenge therefore becomes how to maintain a consistent security and privacy framework around the treatment of that information across legal and jurisdictional borders and geographies.[14]

---

8 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 6–7.

9 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 20.

10 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 7.

11 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

12 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

13 Microsoft, *Submission 14*, p. 5; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1063–65.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1065.

11.9 International frameworks for privacy protection have also been developed in response to the global developments 'to harmonise laws within economic communities and improve trade relationships.' These include the Organisation for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines); European Union (EU) *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (EU Directive); and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[15]

11.10 Currently, NPP 9 provides the specific circumstances in which an organisation can transfer information to a recipient in a foreign country, and is largely modelled on articles 25 and 26 of the EU Directive. There are no requisite arrangements in the Information Privacy Principles (IPPs) which apply to agencies.[16]

11.11 Notably, NPP 9 does not apply where the information is transferred to the same organisation, rather it only applies if the transfer is to a third party. Further, NPP 9 only regulates the transfer of information to 'foreign countries' as opposed to 'other jurisdictions', and therefore:

> It does not protect personal information that is transferred to a state or territory government that is not subject to privacy law, or a private sector organisation that is exempt from the Privacy Act.[17]

11.12 Section 5B of the current Privacy Act ensures that organisations do not avoid their obligations in relation to the management of personal information under the Act by transferring information overseas. The Privacy Act applies to an act or practice relating to personal information about an Australian citizen or permanent resident, and the organisation undertaking the act or practice either has an Australian link or carried on a business in Australia and held or collected information in Australia either before or at the time of the act done or practice engaged in.[18] To implement this, Privacy Commissioner's enforcement powers are extended to overseas complaints which fit specified criteria.[19]

11.13 Subsection 6A(4) and section 13D of the existing Privacy Act provide that an act or practice undertaken overseas which is required by an applicable foreign law will

---

15 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1065–66.

16 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1086–87.

17 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1086–87.

18 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1081–82.

19 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1082.

generally not be taken as a breach of the Act or an interference with the privacy of an individual.[20]

11.14 The ALRC review looked at the following matters, among others:

- international frameworks for privacy protection, in particular, the EU Directive, the APEC Privacy Framework and the Asia-Pacific Privacy Charter;
- regulation of cross-border data flows under the *Privacy Act 1988* via the extraterritorial operation of the Act;
- the restrictions in NPP 9 on the transfer of personal information to countries with differing privacy regimes;
- the content of the 'Cross-border Data Flows' principle in the model Unified Privacy Principles (UPPs) and its application to agencies and related bodies corporate;
- notification requirements; and
- the role of the Privacy Commissioner and the need for Office of the Privacy Commissioner (OPC) guidance.[21]

11.15 The ALRC examined the application of section 5B of the Privacy Act to agencies and formed the view that while section 5B applies only to organisations:

> Agencies often compel the collection of personal information and should therefore remain accountable for the handling of that information under the Privacy Act, whether they are located in Australia or offshore. Further, agencies should not be able to avoid their obligations under the Act by transferring the handling of personal information to entities operating in countries with lower privacy protection standards.[22]

The ALRC therefore recommended that agencies that operate outside Australia should be subject to the Privacy Act.

11.16 One of the criticisms of NPP 9 is that organisations, which transfer personal information to recipients in foreign countries, are not held accountable for subsequent breaches of privacy. Given the risks associated with cross-border transfers, and the significant community concern around the issue, the ALRC suggested it was pertinent that agencies and organisations which transfer information to a recipient outside of Australia be held accountable for the acts and practices of the recipient in respect of

---

20 Explanatory Memorandum, *Privacy Amendment (Private Sector) Bill 2000*, p. 89; Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1084–85.

21 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1066.

22 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1082–1084 and 1104.

the transferred personal information.[23] The ALRC specified three circumstances in which an agency or organisation should not be held liable namely, where the:

- information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the UPPs;
- individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
- agency or organisation is required or authorised to transfer the personal information by or under law.[24]

11.17 The ALRC noted the concerns of stakeholders with respect to the 'reasonably believes' test currently used in NPP 9(a). However, the ALRC recommended that the test be retained, and that the Government issue a list of 'laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar' to those in Australian legislation, to assist agencies and organisations with compliance. The factors to be considered in determining whether an entity has a 'reasonable belief' may include 'the level of enforcement of a relevant law, binding scheme or contract, which may not be answered solely by their inclusion on the proposed list'. Therefore, the ALRC also suggested that the OPC issue guidance on what constitutes a 'reasonable belief'.[25]

11.18 Noting that provision of consent under this principle has significant implications, the ALRC suggested that the application of more detailed consent requirements than the usual 'voluntary and informed', may be required. For example, an agency or organisation may need to be able to demonstrate that informed consent was obtained, possibly through a written acknowledgement. Further, in order to provide informed consent, an individual would need to be notified of the countries to which their information may be sent. Such information could be included in a privacy policy, and the notification requirements under the principles would apply in this circumstance. The ALRC recommended that the OPC provide guidance on what is required of agencies and organisations in obtaining an individual's consent in particular contexts under the Privacy Act.[26]

---

23 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1087–97.

24 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1095–96.

25 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1097–1100.

26 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1103–04.

11.19 The views of submitters to the ALRC review were widely varied on the definition of the term 'transfer' and whether a definition should be provided in the legislation. Given the disparity in views, the ALRC recommended that the OPC issue guidance on the circumstances in which a cross-border transfer would occur, as such guidance 'can more readily be amended to accommodate changes to the ways in which personal information is transferred than a definition of "transfer" under the Privacy Act'.[27]

11.20 Stakeholders noted that under the current legislation it is not clear whether the transfer of personal information outside of Australia to a related body corporate is subject to NPP 9, due to the interaction between this principle and subsection 13B(1). Subsection 13B(1) states that the collection or disclosure of non-sensitive personal information between two related bodies corporate is not an interference with the privacy of an individual. The ALRC formed the view that it is in the public interest for the principle relating to the cross-border transfer of information to apply to transfers of information by organisations to related bodies corporate outside of Australia, as:

> Although many related companies are governed by a common set of internal policies, this may not always be the case. Further, the internal policies of a related company may not always provide the same level of protection as the Privacy Act.[28]

11.21 The ALRC noted that while the 'ability to investigate breaches of local privacy laws in foreign countries poses particular challenges for privacy regulators', the OPC and the Australian Government are already cooperating with privacy regulators in other jurisdictions in various forums.[29]

11.22 Most submitters to the ALRC review stated that an individual should be notified if their personal information will be transferred outside of Australia. However, the ALRC formed the view that a notification each time an individual's information is transferred overseas would be an onerous and unjustified compliance burden on agencies and organisations. The ALRC suggested that it would suffice if:

- the entity's privacy policy set out whether the entity may transfer personal information outside of Australia, and list those countries to which the information may be transferred; and
- under the 'notification' principle, an individual would be notified if their personal information may be transferred overseas.[30]

---

27 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1114–17.

28 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1117–19.

29 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1123.

30 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1127–29.

***Government response***

11.23 The Government accepted seven of the eight ALRC recommendations in relation to cross-border data flows and accepted with amendment the recommendation relating to exceptions.[31]

11.24 In relation to exceptions, the Government accepted that, as a general principle, an agency or organisation should remain accountable for the information which they transfer outside of Australia. The Government was also of the view that there should be certain exceptions to this general principle, agreeing with two of the exceptions proposed by the ALRC, namely the consent exception and the required or authorised by or under law exception. However, the Government considered the exception under which an agency or organisation reasonably believes the recipient is subject to substantially similar privacy protections should be amended to ensure that there are also enforceable mechanisms to enable individuals to take action if there is a breach of their privacy. The Government suggested that these enforcement mechanisms:

> ...may be expressly included in the law or binding scheme or may take effect through the operation of cross-border enforcement arrangements between the Office of the Privacy Commissioner and an appropriate regulatory authority in the foreign jurisdiction.[32]

11.25 The Government also considered that there should be further exceptions to the general principle of accountability, as follows:

- there is a reasonably belief that the disclosure is necessary to lessen or prevent a serious threat to an individual's life, health or safety; or public health or public safety and in the circumstances, it is unreasonable or impracticable to seek the individual's consent;
- there is reason to suspect that unlawful activity or serious misconduct has been, is being, or may be engaged in, and the disclosure of the personal information is a necessary part of the entity's own investigation of the matter or in reporting its concerns to relevant persons or authorities; or
- there is a reasonably belief that the disclosure is necessary for the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law.[33]

11.26 The Government response further stated that individuals should be notified if their personal information is reasonably likely to be transferred overseas, and if so, to

---

31 Australian Government, *Enhancing National Privacy Protection: First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, pp 77–80.

32 Australian Government, *Enhancing National Privacy Protection*, pp 77–78.

33 Australian Government, *Enhancing National Privacy Protection*, p. 78.

which locations it might be transferred. The Government envisaged this requirement would be provided for under the 'notification' principle, and would be qualified by the 'reasonable steps' test (see chapter 8).[34]

## Issues

11.27 The Australian Institute of Credit Management welcomed APP 8 as it believed it will 'significantly ameliorate concerns regarding the management of personal information in the international context'.[35] However, Professor Greenleaf and Mr Waters called APP 8 'the most controversial new principle' as it abandons a 'border protection' approach in favour of an 'approach mis-described as "accountability"'.[36] Privacy NSW considered that the principle should be more stringent than the use or disclosure principle (APP 6) and disclosure should only take place outside Australia where the same level of protection as the APPs is afforded or if there is express consent.[37]

11.28 Other submitters stated that APP 8 increased the compliance burden on organisations, while the Australian Hotels Association commented that this was a further regulatory requirement on an essential business process.[38] Yahoo!7 on the other hand, preferred that accountability for the handling of cross-border data disclosure be through self regulatory codes and cooperative instruments and commented 'whilst we appreciate the need to provide information and reassurance to users in relation to cross-border transfers, we consider any reliance on distinction between borders to be unrealistic'.[39]

11.29 The following discussion addresses concerns in relation to the accountability for personal information transferred overseas, the structure of APP 8, the exceptions to the principle and interaction between APP 8 and section 20.

### *Accountability for personal information transferred overseas*

11.30 The NSW Department of Justice and Attorney General commented that APP 8 itself does not embody the principle of entities remaining accountable for personal information transferred to an overseas recipient. Rather, the principle only provides for a 'reasonable steps' test and the 'accountability' principle is contained in

34 Australian Government, *Enhancing National Privacy Protection*, p. 81.

35 Australian Institute of Credit Management, *Submission 8*, p. 4.

36 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

37 Privacy NSW, *Submission 29*, p. 5.

38 Australian Hotels Association, *Submission 22*, p. 3; Communications Council, *Submission 23*, p. 9.

39 Yahoo!7, *Submission 20*, p. 3.

proposed section 20.[40] The NSW Department of Justice and Attorney General submitted that, for clarity, the accountability principle could be embodied in the APP and not in a separate section of the Act. It was suggested that, at the very least, a note could be included following APP 8 to indicate that the accountability principle applies and stating its location. This would avoid the risk that entities or individuals assuming that APP 8 is exhaustive in relation to cross-border transfers and that the only obligation on entities is to take reasonable steps to ensure that the overseas recipient does not breach the APPs. The NSW Department of Justice and Attorney General went on to submit that compliance only with APP 8 would provide a far more limited safeguard than the accountability principle that appears in section 20.[41] The OPC also supported the inclusion of a note referring to section 20.[42]

11.31 In relation to the change to an 'accountability model', the Australian Bankers Association (ABA) supported APP 8 using such a model as 'it is commercially and socially realistic'.[43] While Google supported the approach in the principle, it voiced concern with the strict liability imposed by section 20.[44] Other submitters also expressed concern about the shift in liability. The Australian Finance Conference (AFC) commented that the principle shifts the risk balance heavily to the entity and queried 'the individual interest justification to support that'. It commented that APP 8 departs from the ALRC recommendations and from the current NPP 9. The AFC also questioned the approach taken in APP 8 given Australia's recent commitment to the APEC Cross-border Privacy Enforcement Arrangement (CPEA). The APEC CPEA is aimed at assisting in the removal of country boundaries in the enforcement of privacy protections.[45]

11.32 Microsoft also raised the CPEA and commented that the combination of APP 8 and section 20 'appears to go further than both the APEC accountability principle and the government's own response to the ALRC recommendations' as the entity will be liable if the recipient outside Australia acts inconsistently with the APPs. Microsoft commented that 'liability will be imposed even where the Australian entity exercised due diligence and took reasonable steps to ensure that the recipient would abide by the principles'.[46]

---

40 As described in paragraph 11.5 above, section 20 makes an entity accountable for the overseas recipient's acts and practices and a breach of the APPs by the overseas recipient will be taken to be that of the entity who disclosed the personal information to the overseas recipient. Companion Guide, p. 13.

41 NSW Department of Justice and Attorney General, *Submission 42*, p. 8.

42 Office of the Privacy Commissioner, *Submission 39*, p. 36.

43 Australian Bankers' Association, *Submission 15*, p. 11.

44 Google, *Submission 16*, p. 7.

45 Australian Finance Conference, *Submission 12*, pp 7–8.

46 Microsoft, *Submission 14*, p. 11; see also Australian Bankers' Association, *Submission 15*, p. 11.

11.33 Deloitte Australia commented on the point raised by Microsoft and suggested that the interaction between section 20 and APP 8 was unclear. Although it supported the accountability principle, Deloitte suggested that the disclosing entity should only be liable under section 20 if it did not take reasonable steps as required under APP 8(1). It also noted the comments of the ALRC in relation to information that is the subject of a contract that effectively upholds privacy protections substantially similar to the UPPs and the provisions of the CPEA.[47]

11.34 The Law Council of Australia (LCA) also commented that the onus placed on entities is stricter than that under the CPEA. The LCA suggested that section 20 is unnecessary if the provisions of APP 8 have been complied with.[48]

11.35 In response to comments in submissions about the intention of the principle, and the shift to an accountability framework, the Department of the Prime Minister and Cabinet (the department) stated that the Government had accepted the general principle that an agency or organisation should remain accountable for personal information that is transferred outside Australia. The Government also accepted that there should be a limited number of exceptions to the principle and that the term 'accountable' should be defined so that the scope of the principle is clear to agencies and organisations.[49]

11.36 The department went on to note that the key instrument considered in developing the principle was the CPEA, which in turn is derived from the OECD principles. The key element of accountability is that an agency or organisation transferring personal information should exercise due diligence and take reasonable steps to ensure the recipient will protect the personal information.

11.37 In addition, one way to meet a requirement that a foreign recipient protect personal information would be to use a contract. The department noted that while contracts will remain useful as important mechanisms for agencies and organisations to impose obligations upon recipients, they should not provide a specific exception on their own from the accountability obligations. It is expected that entities will ordinarily have a contractual relationship with overseas recipients, and that contract would set out the obligations of the overseas recipient. This may not be reasonable in all circumstances but it is the general expectation.[50]

11.38 Matters specific to section 20 are discussed below, see paragraphs 11.121–134.

---

47 Deloitte Touche Tohmatsu, *Submission 28*, pp 1–2.

48 Law Council of Australia, *Submission 31*, p. 6.

49 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 24.

50 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 24.

*Conclusion*

11.39 The committee acknowledges that APP 8 and section 20 address the growing community concerns that technology allows information to be shared freely across borders. While the committee notes concerns about the liability imposed by section 20, even when reasonable steps have been taken by the entity, the department and the Companion Guide explained that this will be managed through contractual relationships with the overseas recipients including privacy obligations. Therefore the committee does not consider that the obligations imposed by APP 8 and section 20 are overly onerous.

11.40 In line with the committee's previous comments in relation to clarity, the committee considers that a note referring to section 20 should be included in APP 8 to ensure that the interaction between both provisions is clear.

**Recommendation 14**

**11.41 The committee recommends that a note be added to the end of APP 8 making reference to section 20 of the new Privacy Act.**

***Notification***

11.42 Professor Graham Greenleaf and Mr Nigel Waters commented that as currently drafted, APP 8 does not appear to require notification of individuals at the time that their data is being transferred to an overseas jurisdiction. They considered that this compounded their concerns raised in relation to APP 1 and APP 5 relating to notification of an individual of the countries to which their personal information may be disclosed.[51]

11.43 The committee notes, that in its review, the ALRC recognised that individuals should be notified if their personal information is to be transferred outside of Australia. However, it was noted that requiring a notification each time an individual's information is transferred overseas would be an onerous compliance requirement for agencies and organisations.[52] The Government agreed with the ALRC's recommendation that an agency or organisation's privacy policy should state whether personal information is likely to be transferred overseas, and where it may be transferred to. The Government also stated in its response that a requirement to notify individuals of the possible transfer of their personal information overseas would be expressly provided for in the 'notification' principle, but would be qualified by a 'reasonable steps' test:

> For example, an agency or organisation would not need to include this information in a collection notice if it did not reasonably know at the time of collection whether information would be transferred overseas.

51 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

52 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1127–29.

> Further, it would not be reasonable to provide specific information if the organisation or agency does not reasonably know to which specific jurisdiction personal information may be transferred.[53]

***Structure and terminology***

11.44 In relation to structure and terminology used in APP 8, the Office of the Victorian Privacy Commissioner (Privacy Victoria), suggested that including exceptions which relate solely to Commonwealth agencies in privacy principles which are supposed to be 'high-level' is problematic, as it increases complexity and makes the principles less readily transferable to states and territories.[54] The AFC also submitted that, as a matter of policy and drafting, APP 8 fails to achieve the key objectives of the privacy reforms of high-level, simple, clear and easy to understand principles.[55]

11.45 Privacy Law Consulting Australia raised various concerns regarding the terminology used in the exposure draft of APP 8. In relation to APP 8(1), it was noted that the APPs do not apply to overseas recipients, therefore phrasing similar to section 20(1)(d) should be included in the provision, such as 'if those Australian Privacy Principles applied to it'.[56]

11.46 The committee has commented on general matters in relation to clarity and agency specific provisions in chapter 3.

*To 'transfer' or to 'disclose'*

11.47 APP 8 uses the term 'disclosure' rather than 'transfer' as is currently used in NPP 9. The Companion Guide states that the term 'transfer' complicates the understanding of the information flow. Rather, the ordinary meaning of disclosure is to allow information to be seen rather than the implication of 'transfer' of a cross-border movement of information. This means that a disclosure will occur when an overseas recipient accesses information, whether or not the personal information that is accessed is stored in Australia or elsewhere. The APP will not apply if the information is routed through servers outside Australia.[57]

11.48 Telstra raised concern about the meaning of 'accessed' by an overseas recipient. While agreeing that the principle should apply in the case where an overseas recipient is able to have possession of personal information, Telstra argued that the principle should not be extended to cover situations in which the information is

---

53 Australian Government, *Enhancing National Privacy Protection*, p. 81. See chapter 8 for further information.

54 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 8.

55 Australian Finance Conference, *Submission 12*, p. 8.

56 Privacy Law Consulting Australia, *Submission 24*, p. 9.

57 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 12.

temporarily 'viewed' by an overseas recipient who cannot print, copy or save the information. In Telstra's opinion, the entity which possesses the information should remain responsible for the management of that information.[58]

11.49 The Financial Services Council (FSC) noted the explanation provided in the Companion Guide, which outlines that information will not be taken to be 'disclosed' if it is routed through servers which are outside of Australia or stored offshore. However, it was submitted that these intentions should be clarified in APP 8 and the provisions of the Privacy Act itself, and explanatory material should also clearly state that entities will need to ensure that information routed or stored offshore is not accessed by third parties, and thereby 'disclosed'.[59]

11.50 The OPC suggested concerns about the use of the term 'disclosure' could be addressed by including explanatory material to note that APP 8 and related provisions only apply to disclosures and not to an entity's internal 'uses'.[60] The OPC also suggested that explanatory material clarifying that APP 8 will apply to disclosures to a 'related body corporate' be included, consistent with recommendations in the ALRC report, and as accepted in the Government's response.[61]

11.51 In relation to the intention that the principle will not apply to information routed through servers outside Australia, the OPC commented that it agreed with this view 'provided the personal information is not accessed by a third party during this process'. The OPC concluded:

> The Companion Guide or other explanatory material could note that entities will need to take a risk management approach to ensure that personal information routed overseas is not accessed by third parties. If the information is accessed by third parties, this will be a disclosure subject to APP 8 (among other principles).[62]

*Conclusion*

11.52 In light of the comments received by the committee in relation to the 'disclosure' of personal information, the committee considers that greater clarity is required around the use of this term. The committee is of the view that explanatory material should be prepared that clearly outlines when information is taken to be 'disclosed' through cross-border activities. The committee also considers that explanatory material regarding the application of APP 8 to disclosures to a 'related body corporate' should be provided.

---

58 Telstra Corporation Limited, *Submission 19*, p. 3.

59 Financial Services Council, *Submission 34*, p. 3; see also Office of the Privacy Commissioner, *Submission 39*, p. 37.

60 Office of the Privacy Commissioner, *Submission 39*, p. 37.

61 Office of the Privacy Commissioner, *Submission 39*, p. 37.

62 Office of the Privacy Commissioner, *Submission 39*, p. 37.

**Recommendation 15**

**11.53 The committee recommends that the Department of the Prime Minister and Cabinet develop explanatory material to clarify the application of the term 'disclosure' in Australian Privacy Principle 8.**

***Ensuring an overseas recipient does not breach the APPs–APP 8(1)***

11.54 APP 8(1) requires an entity, which is disclosing personal information to an overseas recipient, to 'take such steps as are reasonable in the circumstances' to ensure that the overseas recipient does not breach the APPs in relation to the information before the disclosure takes place.

11.55 The LCA submitted that this is an onerous requirement as in order to achieve the aim of APP 8(1) an Australian entity would have to require the overseas entity to bind itself to observe the APPs and the affected overseas entity may resist. The LCA suggested an amendment to the provision so that the Australian entity must take reasonable steps to ensure that the foreign recipient does not hold, use or disclose personal information 'in a manner inconsistent with the Australian Privacy Principles'.[63]

11.56 Qantas expressed concern that the requirement to 'ensure that the overseas recipient does not breach the Australian Privacy Principles' is too broad, suggesting that the approach taken in NPP 9(f), which requires the overseas recipient to hold, use and disclose the personal information in a manner consistent with the APPs, is more appropriate.[64]

11.57 Some submitters commented that APP 8 is complex and confusing, as there is no explanation of what might constitute 'reasonable steps'.[65] Professor Graham Greenleaf and Mr Nigel Waters noted that in the absence of a definition of what might constitute reasonable steps, guidelines from the Australian Information Commissioner are essential. It was further noted that guidance on model contract clauses will make it easier to determine whether a contract meets the 'reasonable steps' compliance test in APP 8(1).[66]

11.58 Dr Colin Bennett argued APP 8 does not explicitly state the intention of the principle, which, as explained in the Companion Guide is that, 'if the overseas recipient does an act or practice that would be a breach, then the entity would be liable'. Dr Bennett suggests that Canadian privacy legislation states the entity's responsibility more clearly, and encourages an organisation to use contractual

63 Australian Law Council, *Supplementary Submission 31a*, p. 4.

64 Qantas, *Submission 38*, pp 7–8.

65 Dr Colin J. Bennett, *Submission 11*, p. 4; Internet Society of Australia, *Submission 41*, p. 3; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

66 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 13.

arrangements to ensure the adequate level of privacy protection is complied with by the third party.[67]

11.59 Coles Supermarkets Australia Pty Ltd (Coles) supported this argument and explained that when outsourcing services, Coles puts contracts in place which oblige the overseas recipient to manage personal information in accordance with the requirements of Australian privacy laws, and provide that the service provider's compliance with the contract may be audited. Coles suggested that similar requirements could be applied under the principles to any third party recipients of personal information, regardless of their location.[68]

11.60 However, in its submission the ABA recognised that it is stated in the Companion Guide that it is generally expected that entities will use contractual arrangements to ensure that an overseas recipient manages information in a manner which is consistent with the APPs, and that the existence of such contractual arrangements indicates that an entity has taken reasonable steps as required.[69]

11.61 Guidance on the term 'reasonable steps', is provided in the *Guidelines to the National Privacy Principles* produced by the OPC, and it is expected that similar guidance will be issued for the APPs. Professor Rosalind Croucher, President of the ALRC, explained that the Office of the Australian Information Commissioner:

> ...might assist in the process of determining what is reasonable, in conjunction with the kinds of other steps that we have suggested before. There are other sources of best practice. The advantage of an information commissioner's office is that it is a central repository and a high-level federal government agency that can assist in the process of making these high-level principles more operationally effective in the interests underpinned by the principles.[70]

11.62 Further, the Government response supported the ALRC's suggestion that the OPC provide guidance on what should be contained in a contractual agreement with an overseas recipient of personal information.[71]

*Conclusion*

11.63 The committee considers that, as the Government envisages that most Australian entities and overseas recipients will have contractual arrangements in place which will be used to ensure information is managed in accordance with Australian privacy law, guidance should be provided to assist entities in this regard. In addition,

---

67 Dr Colin J. Bennett, *Submission 11*, p. 4.

68 Coles Supermarkets Australia Pty Ltd, *Submission 10*, p. 2.

69 Australian Bankers' Association, *Submission 15*, p. 12.

70 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 9.

71 Australian Government, *Enhancing National Privacy Protection*, p. 80.

compliance with APP 8(1) contains a 'reasonable steps' test. Therefore the committee considers that, as a matter of priority, the Office of the Australian Information Commissioner should provide guidance in relation to the type of contractual agreements required to comply with APP 8.

**Recommendation 16**

**11.64 The committee recommends that the Office of the Australian Information Commissioner develop guidance on the types of contractual arrangements required to comply with APP 8 and that guidance be available concurrently with the new Privacy Act.**

***Exceptions***

11.65 APP 8(2) sets out a number of exceptions under which an entity will not be accountable for the cross-border disclosure of personal information to an overseas recipient. As the cross-border disclosure of personal information has been extended to agencies, a number of agency specific exceptions have been included to 'ensure that current information sharing activities of agencies is still permitted'.[72] Comments on the inclusion of agency specific exceptions are contained in chapter 3.

11.66 Professor Greenleaf and Dr Waters argued that the 'attempt at regulation of overseas transfers' through APP 8(1) is 'fatally undermined by APP 8(2) which provides nine separate means by which a data exporter can be exempt from even the theoretical liability/"accountability" of APP 8(1)'.[73] The following canvasses the issues raised in relation to specific exceptions.

*Similar overseas laws and enforcement mechanism exception–APP 8(2)(a)*

11.67 APP 8(2)(a) provides that if the entity transferring personal information overseas 'reasonably believes' that the recipient of that information is subject to laws which protect the information in a way that is at least substantially similar to the APPs and there are accessible mechanisms available to enforce those protections, an exception to the provisions of APP 8(1) is available.

11.68 Microsoft noted the Government's response to the ALRC's recommendations extended the exception to include the accessible enforcement mechanisms for individuals to be able to take effective action to have the privacy protections enforced. The Government response stated that any such enforcement mechanism may be expressly provided for in a law or binding scheme, or be given effect through cross-border enforcement arrangements between the OPC and an appropriate foreign regulator. Microsoft submitted that it did not consider that proposed APP 8(2)(a) reflects the position stated in the Government response. Microsoft suggested that the exception be redrafted to ensure that:

---

72 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

73 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

- the foreign recipient is in a jurisdiction with an adequate level of protection;
- the foreign recipient is in a jurisdiction that has entered into a cross-border enforcement arrangement with the OPC that will enable an individual to pursue a claim against the foreign recipient in respect of conduct that would constitute an interference of privacy if it had occurred in Australia.[74]

11.69 A number of other issues were raised in relation to this exception. On the one hand, privacy commentators considered that the exception was flawed while data exporters pointed to the compliance burden.

11.70 Professor Greenleaf and Mr Waters argued that APP 8(2) was weakened by the inclusion of the term 'reasonably believes' and submitted that:

> Some organisations will inevitably make self-serving judgements about the level of protection in other jurisdictions and/or pay for advice that supports their desire to transfer. Similar protection should be an exception to any prohibition on transfer, but it must be based on objective criteria.[75]

11.71 As a consequence, they recommended that the term 'the entity reasonably believes that' be deleted, 'so that the question of the effectiveness of the overseas privacy protections becomes a question of fact, to be determined initially by the Privacy Commissioner on the basis of a complaint, and ultimately by a court on appeal'. Professor Greenleaf and Mr Waters concluded that 'such ex post facto determinations may discourage exports of Australians' personal information to countries where privacy protection is questionable, but that would be a good result'.[76]

11.72 Dr Colin Bennet was of a similar view: either the overseas recipient is subject to a law or binding scheme similar to the Australian legislation, or it isn't, and noted that entities could use this to avoid liability in cases where they have not exercised due diligence.[77]

11.73 Submitters raised concerns in relation to the compliance burden and access to a comprehensive list of destinations which have regimes so that an entity could comply with APP 8(2)(a). Qantas, for example, submitted that the requirements of APP 8(2)(a) relating to the availability of enforcement mechanisms is 'too onerous for an Australian entity to comply with and should be removed'.[78] In addition, it was argued that if entities were required to make their own determination, a situation could

74 Microsoft, *Submission 14*, p. 11.

75 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

76 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

77 Dr Colin J Bennett, *Submission 11*, p. 4.

78 Qantas, *Submission 36*, p. 8; see also Telstra Corporation Limited, *Submission 19*, pp 3–4.

arise whereby different entities make different determinations about the level of privacy protection available in various jurisdictions.[79]

11.74 Submitters called for the provision of a list which identifies countries with similar privacy laws to Australia and which have accessible protection mechanisms. Submitters suggested that the OPC should compile and publish a list while Microsoft suggested that this should be a 'positive obligation' on the OPC.[80] Such as list would ensure consistent treatment of privacy protection between entities and would assist entities in complying with their obligations, particularly under APP 8(2)(a) when disclosing information offshore.[81] It was noted that some international jurisdictions have adopted this approach in relation to Anti-Money Laundering legislation, and that the compilation of such a list may be facilitated by the new APEC Cross-border Privacy Enforcement Arrangement.[82]

11.75 The NSW Department of Justice and Attorney General also commented that the NSW Law Reform Commission's view was that, if such a list is published, there is no need for the reasonable belief test. Further, such a list could include not only laws but also 'binding schemes' such as inter-governmental agreements or effective self-regulatory schemes. The NSW Department of Justice and Attorney General stated:

> There is a question about the circumstances in which an entity could hold the necessary "reasonable belief" in relation to an entity in a jurisdiction not on the list. It is conceivable that a jurisdiction with adequate protection might not be on the list due to delays in maintaining the list. In such circumstances, the reasonable belief test could provide a safety net for entities. However, provided the list is effectively created and maintained, in the vast majority of cases a belief is unlikely to be 'reasonable' in relation to an entity in a non-listed jurisdiction.[83]

11.76 The NSW Department of Justice and Attorney General further commented that a belief may be reasonable, based on the information available to an entity, but it may be ill informed and incorrect. It concluded that removal of the 'reasonable belief' exception in favour of the 'listed jurisdiction' approach, as recommended by the NSW Law Reform Commission may be worth further consideration.[84]

---

79 Telstra Corporation Limited, *Submission 19*, p. 4.

80 Microsoft, *Submission 14*, p. 12.

81 The Westpac Group, *Submission 13*, p. 3; Australian Bankers' Association Inc., *Submission 15*, p. 13; Telstra Corporation Limited, *Submission 19*, pp 3-4; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14; Deloitte Touche Tohmatsu, *Submission 28*, p. 2.

82 The Westpac Group, *Submission 13*, p. 3; Internet Society of Australia, *Submission 41*, p. 3; Telstra Corporation Limited, *Submission 19*, pp 3–4.

83 NSW Department of Justice and Attorney General, *Submission 42*, p. 9.

84 NSW Department of Justice and Attorney General, *Submission 42*, p. 9.

11.77 The ALRC review recognised concerns regarding the 'reasonably believes' test which is used in existing NPP 9(a), but recommended that the test be retained. To assist agencies and organisations with compliance, the ALRC suggested the Government issue a list of laws and binding schemes which are substantially similar to the protections provided under Australian legislation. However, the ALRC noted that the level of enforcement of a relevant law or binding scheme would not be reflected by inclusion on a list. For example, entities may know that there is no mechanism for enforcement of privacy protection laws and thus could not demonstrate 'reasonable belief' for the purposes of the principle. The ALRC suggested that the OPC issue guidance on the 'cross-border data flows' principle which should include what constitutes a 'reasonable belief'.[85]

11.78 In its response to issues raised in relation to this exception, the department noted that 'the ALRC made it clear that the mere fact that a recipient is subject to a listed binding law or scheme is not determinative in itself, as the entity must still form its own reasonable belief based on the information available to it'. Further, the Government response stated that agencies and organisations will be able to use the list to assist them in forming a reasonable belief that, in the circumstances of their particular cross-border transfer of personal information, the recipient of the information will be accountable. The department commented:

> Once armed with the initial information, entities would be in the best position to find out about the specific laws that apply to the overseas recipient, including whether the recipient is bound by existing privacy laws in the overseas jurisdiction that are substantially similar (we understand that some privacy laws, for example in Korea, only apply to certain industry sectors).[86]

11.79 The department noted that the list would be prepared by the Government rather than the Office of the Australian Information Commissioner.[87]

11.80 The enforcement mechanism requirement was also examined by the LIV from the perspective of access by affected individuals. While mechanisms may exist, the LIV commented that if it is time consuming, costly, or not applied in a practical sense 'then it does not provide any meaningful protection to individuals' and 'it is unrealistic to expect Australian citizens to avail themselves of such mechanisms'.[88] PIAC and the Health Services Commissioner similarly argued that the affected individual should not have to take action in another jurisdiction against a third party in order to protect the rights afforded by Australian privacy law. Rather, the individual should always be

---

85 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1097–1100.

86 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 25.

87 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 25.

88 Law Institute of Victoria, *Submission 36*, p. 7.

able to take action in Australia and against the entity with which he or she had direct dealings.[89]

*Consent to cross-border disclosure–APP 8(2)(b)*

11.81 APP 8(2)(b) provides that APP 8(1) does not apply if the entity obtains the consent of the individual to overseas disclosure, after the individual has been given information to that effect. Submitters raised two matters: the practicality of the consent requirement in relation to commonplace international transactions; and the lack of the need to gain 'express' consent.

11.82 The ABA noted that there are a wide range of quite common international transactions, such as international payments and international credit card transactions, in which it is clear that information will cross international borders. The ABA stated that it is not practicable to impose controls on recipients in such transactions, and consequently, its members will find it difficult to meet the requirements under APP 8(2)(b). To address this issue, the ABA suggested an additional exception be provided under APP 8(2) for circumstances in which the:

> ...overseas transfer of information is a necessary step in providing a service which would be obvious to a reasonable person turning their mind to the circumstances.[90]

11.83 The ABA submitted that if a bank is required to expressly inform each individual customer separately that their information will be disclosed to an overseas recipient, 'the consent exception will, in all practicality, be illusory'. Consequently, the ABA suggested that an individual can be expressly informed by an entity through the provision of information in the entity's privacy policy, so that the customer is aware that in continuing to deal with the entity, they consent to the potential for their information to be sent to an overseas recipient.[91]

11.84 However, the possibility that entities would use privacy statements to meet the consent requirement was of concern to other submitters. Professor Greenleaf and Mr Waters commented that there was no requirement to explain the 'risk' either generally or in relation to a specific destination. As consent can be implied, entities may rely on 'small print' notices in standard terms and conditions statements which were 'completely ineffective'.[92]

11.85 The issue of 'implied' consent through a notice being included in a privacy statement was raised by other submitters.[93] The Health Services Commissioner,

---

89 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 3; Public Interest Advocacy Centre, *Submission 32*, p. 1, Attachment, pp 12–13.

90 Australian Bankers' Association, *Submission 15*, p. 12.

91 Australian Bankers' Association, *Submission 15*, pp 12–13.

92 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15, Attachment, p.15.

93 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 3.

Victoria, argued that a detailed privacy notice at the end of a document which includes information about disclosures overseas 'is not likely to be read by many individuals'. In addition, more stringent requirements are needed in relation to sending health information overseas.[94] The LIV suggested that if this provision is retained, it should incorporate a requirement that such consent be 'free, express and fully informed' to ensure that any such consent is not implied.[95] Professor Greenleaf and Mr Waters suggested that the provision be amended so that individuals, who consent, be provided with a written notice that contains the information provided to the individual when the consent was given.[96]

11.86 In its review, the ALRC considered that the application of more detailed consent requirements than the usual 'voluntary and informed', may be required under this principle as provision of consent in these circumstances has significant implications. Consequently, the ALRC recommended that the OPC provide guidance on what is required of agencies and organisations in obtaining an individual's consent to the transfer of their information overseas. This recommendation was accepted by the Government.[97]

11.87 The ALRC's position on the concept of consent was explained more fully by Professor Rosalind Croucher, President of the ALRC at the committee's public hearing:

> In our report we recommended that the Office of the Privacy Commissioner should develop and publish guidance about what is required of agencies and organisations to obtain an individual's consent. This guidance should, for instance, address a number of the things that I am grabbing at—the factors to be taken into account by agencies and organisations in assessing whether it has been obtained, which is kind of what you are asking about in asking how. It should cover express and implied consent as it applies in various contexts and include advice on when it is and is not appropriate to use the mechanism of bundled consent—in other words, a consent to general use. So we do consider that in the report. I suppose the simple answer is that it depends on the context, but we have suggested that the Office of the Privacy Commissioner, which now sits under the Information Commissioner's office, might be the appropriate agency through which such guidance could be developed.[98]

---

94 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 3.

95 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 8; see also Privacy NSW, *Submission 29*, p. 5.

96 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15, Attachment, p.15.

97 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 1103–04; Australian Government, *Enhancing National Privacy Protection*, p. 80.

98 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 7.

*Required or authorised by or under and Australian law–APP 8(2)(c)*

11.88 Google Australia Pty Limited (Google) suggested that APP 8(2)(c) only covers disclosures to an overseas recipient, not any subsequent disclosure by that recipient which may be required by law in the overseas jurisdiction. It was argued that the provision should recognise requirements of foreign law to ensure that Australian entities are not put at risk of being in breach of the Act under section 20, due to a disclosure of personal information by an overseas recipient required by a foreign law.[99]

11.89 However, the committee notes that the Companion Guide indicates that subsection 6A(4) and section 13D of the current Privacy Act, provide that if an act or practice which is done or engaged in outside Australia is required by an applicable law of a foreign jurisdiction, then that act or practice is not deemed to be an interference with privacy. The Companion Guide states that these provisions are to be replicated in the new Act and will cover agencies.[100] In addition, the department responded to Google's concerns and reiterated that the existing policy achieved by subsection 6A(4) and section 13D of the Privacy Act will be retained in the amended Act. In the example provided by Google, an Australian entity would not breach the APPs if an applicable foreign law required disclosure of personal information by an entity to which that information had been disclosed.[101]

*Required or authorised by or under an international agreement–APP 8(2)(d)*

11.90 APP 8(2)(d) provides an exception if an entity is an agency and the disclosure of the information is required by or authorised by or under an international agreement related to information sharing, and Australia is a party to that agreement. Concerns were raised by the LIV that compliance with the APPs may be avoided by government by entering international agreements. The LIV stated 'we note that there is no regulation or requirement that international agreements about information sharing comply with the APP' and provided the example of the ease with which governments can circumvent the APPs through international agreements by pointing to the Department of Immigration and Citizenship's agreement with five countries to exchange biometric information in relation to protection visa applicants.[102] Professor Greenleaf and Mr Nigel Waters went further and called this 'policy laundering', that is 'hiding behind often spurious claims of "international obligations" to justify actions which would not otherwise be lawful'.[103]

99 Google Australia Pty Limited, *Submission 16*, pp 7–8.

100 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 7.

101 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 25.

102 Law Institute of Victoria, *Submission 36*, p. 7.

103 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 15.

11.91 The OPC expressed similar concerns that the scope of the exception was unclear and could be quite widely interpreted, thereby limiting the circumstances in which an agency can be held accountable for the disclosure of personal information overseas. The OPC explained that wherever practicable 'specific domestic legislative authority should be the basis for an agency to disclose personal information under an international agreement relating to information sharing' thereby providing clarity and certainty to agencies and ensuring that information sharing practices by agencies are subject to appropriate parliamentary scrutiny. If no such legislative authority exists, the OPC suggested the disclosure of information should be subject to other forms of scrutiny, 'such as through a public interest determination (a legislative instrument) issued by the Privacy Commissioner'.[104]

11.92 With regard to this exception, OPC suggested the committee:

- seek further advice on the range of international agreements that may be encompassed by the exception; and
- consider whether those agreements are subject to sufficient parliamentary scrutiny, such that it is appropriate for APP 8 to permit disclosures that are authorised by those agreements (rather than relying on the 'required or authorised by law' exception in APP 8(2)(c)).[105]

11.93 The Companion Guide states that the exception allowing cross-border disclosure of information pursuant to information sharing under an international agreement, was necessary to include as the cross-border disclosure principle has been extended to cover agencies. This exception will facilitate the current information sharing activities of agencies.[106]

*Law enforcement activities–APP 8(2)(g)*

11.94 An exception is available to agencies for the disclosure of information, to overseas bodies 'similar' to Australian enforcement bodies, where it is necessary for law enforcement activities by, or on behalf of, an Australian enforcement body. The OPC commented that the requirement that the overseas body performs functions, or exercises powers similar to those performed or exercised by the Australian body could be broadly interpreted. The OPC suggested that the term 'substantially similar' be used instead, as the definition of an enforcement body is strictly defined in section 15 of the exposure draft.[107]

104 Office of the Privacy Commissioner, *Submission 39*, p. 38.

105 Office of the Privacy Commissioner, *Submission 39*, p. 38.

106 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, p. 13.

107 Office of the Privacy Commissioner, *Submission 39*, pp 38–39.

*Diplomatic, consular and defence activities–APP 8(2)(h) and APP 8(2)(i)*

11.95 As noted in chapter 3, the OPC recommended that the diplomatic, consular and Defence Force activities exceptions be addressed in portfolio legislation rather than the Privacy Act, ensuring that these exceptions are only invoked where appropriate. Consequently the APPs would remain a broad high-level framework, applicable to all entities.[108]

*Exceptions no longer included in the cross-border principle*

11.96 The Law Council of Australia and Qantas noted that two exceptions which are currently provided for under the NPPs have not been included in APP 8. These relate to when the transfer of information is necessary under a contract (NPP 9(c) and (d)). In effect, the absence of these provisions means that:

> ...if an entity needs to disclose personal information which is necessary for the conclusion of the contract with an overseas entity which is not subject to a scheme which is similar to the APPs the entity will need to obtain consent or to enter into a contract which will ensure the overseas recipient does not breach the APPs.[109]

11.97 It was noted that this would be impracticable in a number of circumstances, particularly in sectors such as the travel industry. In such industries, entities commonly deal with overseas organisations with whom it is impracticable to enter into a contract, and situations in which it would not be possible to obtain an individual's consent at short notice. For these reasons, the Law Council and Qantas recommended that the NPP exceptions relating to the transfer of information required under a contract be included in the APPs.[110]

11.98 The department stated that in partially adopting ALRC recommendation 31-2, the Government accepted that it was not necessary to include an exception relating to fulfilling contractual obligations. In recommendation 31-2, the ALRC stated that, under the 'Cross-border Data Flows' principle, an exception to the concept of accountability should include where an agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model Unified Privacy Principles. The department went on to state:

> The Government response to ALRC recommendation 31-2 stated that the application of contractual obligations on the recipient of the information does not provide an individual with any rights to take action under the contract. It went on to comment that, while contracts are important mechanisms for agencies and organisations to impose obligations upon

---

108 Office of the Privacy Commissioner, *Submission 39*, pp 28–30 and 39.

109 Law Council of Australia, *Submission 31*, p. 6; Law Council of Australia, *Supplementary Submission 31a*, p. 4; Qantas, *Submission 38*, pp 7–8.

110 Law Council of Australia, *Submission 31*, pp 6–7; Qantas, *Submission 38*, pp 7–8.

> recipients, they should not provide an exception from the general accountability obligations.
>
> Further, it is clear that in the case of existing NPP 9(c) and (d), which involves a contract between the individual and the organisation, or a contract concluded in the interest of the individual between the organisation and a third party, that the individual would consent to the transfer of the information. Under the new APP 8(2)(b), consent of the individual is an exception to the general prohibition under APP 8(1).[111]

*Conclusions*

11.99 The committee considers that it is reasonable to include exceptions to APP 8 in particular circumstances. The first exception, APP 8(2)(a), provides for an exception where similar law and enforcement mechanisms apply to the overseas recipients. The ALRC recognised that one of the more significant challenges faced by privacy regulators, is the ability to investigate breaches of local privacy laws in foreign countries. In light of this, the Government considered it appropriate that any law or binding scheme deemed to be substantially similar to the APPs must have effective enforcement mechanisms in order to be subject to the exception to the general accountability obligation. The Government suggested that such enforcement mechanisms could be specifically included in the law or binding scheme, or 'may take effect through the operation of cross-border enforcement arrangements between the Office of the Privacy Commissioner and an appropriate regulatory authority in the foreign jurisdiction.' The committee notes that the OPC and the Australian Government are already working to improve cooperative arrangements between privacy regulators across jurisdictions in a variety of forums including the CPEA.[112]

11.100 In relation to recommendations that a list of jurisdictions with similar privacy schemes be provided, the committee notes the department's comments that the list will be provided by the Government. However, the Government's expectation is that this will be 'initial information' and that entities will 'be in the best position' to find out about specific laws that apply to the overseas recipients they are dealing with. While the committee acknowledges that as it is the entity that is transferring the personal information overseas, it must be of a reasonable belief that the overseas jurisdiction provides for similar privacy protections, it may not always be possible for an entity to make such a judgment. The committee therefore considers that the Office of the Australian Information Commissioner should be available to assist entities in the interpretation of overseas privacy laws.

11.101 The committee considers that the 'consent' to cross-border transfers of personal information provides entities with a significant exception. As such, the

---

111 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 26.

112 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 1123; Australian Government, *Enhancing National Privacy Protection*, pp 77–78.

11.102 The committee has some concerns with the exception provided to agencies under APP 8(2)(d)–required or authorised by or under an international agreement. The committee considers that the scope of this exception is unclear and in addition, notes comments about its potential to undermine accountability and scrutiny. While the Parliament has formal mechanism to refer treaties to the Treaties Joint Standing Committee, this committee does not review sub treaty level agreements. The committee therefore considers that use of this exception by agencies should be subject to accountability mechanisms and parliamentary scrutiny.

**Recommendation 17**

**11.103 The committee recommends that, when the Australian Government enters into an international agreement relating to information sharing which will constitute an exception under APP 8(2)(d), the agency or the relevant minister table in the Parliament, as soon as practicable following the commencement of that agreement, a statement indicating:**

- **the terms under which personal information will be disclosed pursuant to the agreement; and**
- **the effect of the agreement on the privacy rights of individuals.**

11.104 In relation to the exception for law enforcement activities, the committee notes the OPC's concerns that APP 8(2)(g) could be interpreted broadly and suggests that the wording of this provision be revisited.

**Recommendation 18**

**11.105 The committee recommends that further consideration be given to the wording of the law enforcement exception in APP 8(2)(g) to ensure that the intention of the provision is clear.**

***Extra-territorial application of the Privacy Act –section 19***

11.106 Section 19 provides for the extra-territorial operation of the Act, that is the APPs will apply if the agency or organisation has an Australian link.

11.107 Google Australia Pty Limited (Google) agreed with the concept of 'Australian link' provided for in the exposure draft, and Professor Greenleaf and Mr Waters expressed support for the provision enabling the Privacy Commissioner to investigate acts and practices which occur outside of Australia.[113] The Australian Direct Marketing Association (ADMA) and Professor Greenleaf and Mr Waters supported

113 Google Australia Pty Limited, *Submission 16*, p. 6; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 4.

the extension of the protection under the extra-territoriality provision to cover the personal information of those who are not Australian citizens or permanent residents.[114]

11.108 Some submitters noted that paragraph 19(3)(g), does not clearly state where collection is deemed to have taken place.[115] The OPC provided comments in relation to the collection of information in the online context. The OPC pointed to the case where a person in Australia provided information to an overseas-based organisation. The OPC suggested that subsection 19(3) could clarify that:

> ...the Privacy Act applies to overseas acts or practices where the personal information is collected from or held in Australia. This may help to clarify that the Act applies where personal information is collected via the internet from an individual who is physically in Australia. There may also be alternative ways to clarify that personal information 'collected or held in Australia' includes such information collected over the internet.[116]

11.109 The OPC concluded that clarifying the scope of extra-territorial operation of the Privacy Act would enhance the Office's ability to apply the Act in these circumstances.[117]

11.110 Alternatively, two submitters suggested that, given that it is often difficult to ascertain the location of the user, the place of collection should be 'the place at which the information is collated and processed', therefore the provision should make it clear that:

> ...information is "collected" at the place (that is, in the jurisdiction) of the service provider collecting the information, not the place where the user is or may be presumed to be at the time that the information is collected.[118]

11.111 In its answers to questions on notice, the department commented that international internet services, such as entities engaged in online retail that sell to Australians, would be required to comply with the APPs so long as they fulfilled both branches of paragraph 19(3)(g). The department went on to state:

> It is likely that sub-paragraph 19(3)(g)(i) would capture businesses operating in Australia, but not businesses operating in foreign jurisdictions that happen to engage in commerce incidental to their primary purposes with customers in Australia.

---

114 Australian Direct Marketing Association, *Submission 27*, p. 8; Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 4.

115 Google Australia Pty Limited, *Submission 16*, p. 6; Office of the Privacy Commissioner, *Submission 39*, pp 43-44; Law Council of Australia, *Submission 31*, p. 9.

116 Office of the Privacy Commissioner, *Submission 39*, p. 44.

117 Office of the Privacy Commissioner, *Submission 39*, p. 44.

118 Google Australia Pty Limited, *Submission 16*, p. 6; Law Council of Australia, *Submission 31*, p. 9.

> Collection takes place for the purpose of the Act when data is entered in Australia, regardless of the point of collation or processing. As such, the place of collection affects whether the Act applies, and once collection takes place s20, which sets out rules and responsibilities relating to the disclosure of personal information to an overseas recipient would apply with regard to acts or practices concerning the data collected.[119]

*'Australian link'*

11.112 Three submitters expressed concerns with the extension of the extra-territoriality provisions under section 19, as in practice this would mean that organisations with an Australian link, and every subsidiary or related body corporate of such organisations, will be subject to the APPs regardless of whether the information they are processing 'does not touch Australia and does not relate to the personal information of an individual in Australia.'[120] Each submitter suggested different options for limiting the application of the extra-territoriality provisions:

- the Law Council recommended that the Act should only extend to the acts and practices of an organisation under paragraph 19(3)(g) which relate to 'personal information that was collected or held in Australia by the organisation, or personal information about an Australian citizen or a permanent resident';[121]
- ADMA recommended that the extra-territoriality provisions be limited to apply only to companies with a presence in Australia;[122] and
- the FSC suggested that the APPs should not apply to 'information collected overseas by an entity that operates in Australia.'[123]

11.113 Further, the OPC raised concerns that the definition of 'Australian link' in the exposure draft differs slightly to the existing definition under the current legislation. The OPC noted that:

> As it refers to 'personal information' generally, it does not appear to require that 'the' specific item of personal information that is involved in a particular overseas act or practice was collected or held in Australia. This may unintentionally imply that, once an organisation collects or holds any personal information in Australia, an individual located overseas could complain under the Privacy Act about the organisation's acts or practices outside Australia, in relation to any personal information the organisation

119 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 30.

120 Law Council of Australia, *Submission 31*, pp 8–9. See also Australian Direct Marketing Association, *Submission 27*, p. 8; Financial Services Council, *Submission 34*, p. 3.

121 Law Council of Australia, *Submission 31*, pp 8–9.

122 Australian Direct Marketing Association, *Submission 27*, p. 8.

123 Financial Services Council, *Submission 34*, p. 3.

> holds about the individual (even if that information was never collected or held in Australia).[124]

11.114 The LIV noted that, under section 19 of the exposure draft, the APPs will apply to an organisation with an Australian link, however, under the current Privacy Act, the NPPs apply to an organisation if the act or practice relates to the personal information of an Australian citizen or permanent resident. The LIV expressed concern that the change of emphasis in the exposure draft may result in a reduction of protection for Australian citizens and permanent residents, particularly if they provide information to an agency which does not have an Australian link.[125]

11.115 The LCA also noted that while the current provisions stating that an act or practice required by an applicable law of a foreign country will not be taken as an interference with privacy will be replicated in the new Act, the existing provision, 'only applies to acts or practices required by foreign law (i.e. response to subpoena or other legal compulsion), not acts permitted in that jurisdiction.'[126]

11.116 The LCA expressed concern that:

> Disclosure under compulsion of Australian law is permitted, but not disclosure under compulsion of foreign law. This compounds the problem noted above, as (for example) a US office of an Australian corporation responding to US court process could find itself in jeopardy under Australian law (again, even if the data subject was not an Australian person or a person living in Australia). The Committee recommends that disclosures required under any law or legal process applicable to the organisation should be expressly permitted.[127]

11.117 The department responded to the LCA's concerns and stated:

> The exposure draft APPs is just one part of the process of amending the Privacy Act. As noted above, the Government intends for disclosure by organisations with an Australian link (as per s 19(3)) under foreign law to be a valid exemption from the operation of s 9(1).
>
> Provisions for the operation of foreign law in this way are currently enacted in section 13D of the Privacy Act. Since the policy intent behind these provisions has not changed, they have been replicated in the new APPs. Some minor issues relating to the definition of the law of a foreign country need to be resolved before this takes place, but these will be further revised in the reforms before they are brought before the Parliament.[128]

---

124 Office of the Privacy Commissioner, *Submission 39*, p. 43.

125 Law Institute of Victoria, *Submission 36*, p. 9.

126 Law Council of Australia, *Submission 31*, pp 8–9.

127 Law Council of Australia, *Submission 31*, pp 8–9.

128 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 30.

*Conclusion*

11.118 In relation to the concerns raised by the LCA, the committee notes that as stated in the Companion Guide, the policy achieved by subsection 6A(4) and section 13D of the *Privacy Act 1988*, will be replicated in the new Act ensuring that if an act or practice is required by an applicable law of a foreign country, it will not be taken as an interference with privacy.

11.119 The committee supports the concept of 'Australian link' as provided for in section 19. The committee notes that the policy intent that for a person to complain about the management about their personal information, that information must be held in Australia or collected in Australia. However, the committee has noted that there are concerns that this policy intent is not adequately expressed in proposed section 19. The committee therefore considers that further clarification on this matter is required.

**Recommendation 19**

**11.120 The committee recommends that section 19, relating to the extraterritorial application of the Act, be reconsidered to provide clarity as to the policy intent of the provision.**

***Acts and practices of overseas recipients of personal information–section 20***

11.121 Concerns were raised about the liability imposed on an Australian entity for the actions of an overseas entity, particularly, as under section 20 an entity is subject to strict liability even if it has taken all reasonable steps to ensure the overseas recipient complies with the APPs.[129] The AFC noted that section 20 only applies if information is disclosed to an overseas recipient under APP 8(1), but doesn't apply if the information is disclosed under APP 8(2). As a result, if information is disclosed to an overseas recipient under APP 8(2), it is the overseas recipient that remains liable, not the disclosing entity.[130]

11.122 The ABA considered this provision to be 'unreasonable' while Telstra noted that even if the entity takes all reasonable steps, there is still the possibility that the entity will not comply, which the Australian entity cannot prevent.[131] The Australian Association of National Advertisers noted that in some cases entities may have recourse through a contract but pointed to instances where, for example, an overseas recipient's computers are hacked. The AANA suggested that the provision is unfair if

129 Microsoft, *Submission 14*, p. 11; Australian Bankers' Association, *Submission 15*, p. 11; The Communications Council, *Submission 23*, p. 8; Deloitte Touche Tohmatsu, *Submission 28*, pp 1–2; Google Australia Pty Limited, *Submission 16*, p. 7; Law Council of Australia, *Submission 31*, p. 9.

130 Australian Finance Conference, *Submission 12*, pp 7–8.

131 Telstra, *Submission 19*, p. 5.

provision is not made for mitigating factors for example, personal information was obtained through hacking.[132]

11.123 The committee was provided with a range of suggestions to address the concerns raised:

- the LCA recommended where the disclosure complies with APP 8, the entity should not be liable for any acts done, or practices engaged in, by the overseas recipient in relation to that information;[133]
- the ABA suggested subsection 20(2) be qualified to limit application of the phrase 'for the purposes of this Act' to refer to the purposes of the compensation provisions of the Act, rather than the penalty provisions of the Act;[134]
- Telstra suggested that section 20 impose an obligation on an entity to 'use reasonable endeavours to ensure that the overseas recipient remedies any act or omission that would otherwise constitute a breach of the APPs';[135] and
- the AANA suggested that section 20 be amended to include exemptions to deal with mitigating factors.[136]

11.124 The department responded specifically to the AANA's comments and noted that unauthorised disclosure of personal information that has been lawfully transferred to a foreign entity via a breach of that foreign entity's data security would not, under the new Privacy Act, be a breach of section 20 as the breach and disclosure would not be an 'act or practice' of the foreign entity. The department added:

> The accountability of organisations which choose to transfer data across borders as provided for in s 20 is a necessary condition for the security of that data. Contracts in place between two entities involved in a cross-border transfer of data do not provide adequate protections for the individuals to whom the information pertains. As such, contracts are not an acceptable mitigating factor for the purposes of s 20.[137]

11.125 The LCA raised further concerns that the exposure draft does not specify a time period after which an entity is no longer liable for the acts or practices of an overseas recipient. In light of this, the LCA suggested that the liability imposed by section 20 be limited in time and aligned with other statutory limitation periods.[138]

---

132 Australian Association of National Advertisers, *Submission 21*, p. 8.

133 Law Council of Australia, *Submission 31*, p. 9.

134 Australian Bankers' Association, *Submission 15*, p. 11.

135 Telstra, *Submission 19*, p. 5.

136 Australian Association of National Advertisers, *Submission 21*, p. 8.

137 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 31.

138 Law Council of Australia, *Submission 31*, p. 10.

11.126 Further, the ABA voiced concern that an overseas data custodian, which has breached the APPs, may be able to limit its liability to the Australian data collector under Australia's proportionate liability laws.[139] The department commented on this point and noted that there is not currently any statutory limitation relating to the 'interference of privacy' that may occur under section 20. As the Act has not previously envisaged judicial enforcement (consistent with the principles-based nature of the Privacy Act), limitation periods have not been a relevant factor.

11.127 The department added that the ALRC has made a number of recommendations that the Australian Information Commissioner be given stronger enforcement powers, for example, the power to commence proceedings in the Federal Court or Federal Magistrates Court for enforcement orders and civil penalties. The department concluded:

> The Government has either accepted, or accepted in-principle, these recommendations, and will be developing draft amendments to address these issues. Relevant civil litigation rules that underpin this system, including statutory limitation periods, will be considered as part of the development of these amendments.[140]

11.128 Professor Greenleaf and Mr Waters questioned the ability of individuals to prove that a breach of the APPs has occurred in an overseas jurisdiction. They submitted that section 20 should be amended to provide that:

> ...a breach by an overseas recipient should be a rebuttable presumption if damage to the individual can reasonably be assumed to have resulted from the export.[141]

11.129 Telstra requested clarification regarding the possible application of APP 8 and section 20 to personal information which has been lawfully published. Telstra noted concern that if an overseas recipient accessed publicly available personal information, the entity which lawfully published the information might be held liable under section 20 for any inappropriate use of the information by an overseas recipient.[142]

11.130 The National Australia Bank (NAB), noted that it is unclear from the exposure draft how APP 8 and section 20 interact if the APPs apply to the overseas recipient, for example, if the overseas recipient is an entity with an Australian link. According to NAB, it appears that section 20 would not apply in these circumstances, however under APP 8(1) the entity would still have to undertake reasonable steps to ensure that the overseas recipient doesn't breach the APPs. Consequently NAB

---

139 Australian Bankers' Association, *Submission 15*, pp 11–12.

140 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 31.

141 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 14.

142 Telstra Corporation Limited, *Submission 19*, p. 4.

submitted that section 20(1) and APP 8(1) should be made consistent to avoid confusion.[143]

11.131 The LIV raised a similar issue with regards to the interaction between APP 8 and section 19:

> APP 8(2)(a)(i) states that an entity is not bound to take reasonable steps to ensure that an overseas recipient of personal information collected in Australia does not breach the APPs if the entity reasonably believes that the overseas recipient is subject to a law or binding scheme that protects privacy in a 'substantially similar way'. Clause 19, however, intends to extend the application of the *Privacy Act 1988* (Cth) to an act done, or practice engaged in, outside Australia by an organisation that has an 'Australian link'. The LIV queries which provision prevails in circumstances where an overseas entity is captured by both APP 8 and cl 19.[144]

*Conclusion*

11.132 The committee received a range of comments in relation to section 20 in particular the application of the section in practice. The committee considers that further clarification is required, for example, through explanatory material to accompany the legislation.

**Recommendation 20**

**11.133 The committee recommends that the Department of the Prime Minister and Cabinet develop explanatory material in relation to the application of the accountability provisions of section 20.**

11.134 The committee also notes that the department has indicated that the Government has accepted the ALRC's recommendations in relation to stronger enforcement powers for the Australian Information Commissioner. The committee awaits with interest the exposure draft relating to the powers and function of the Information Commissioner.

143 National Australia Bank, *Submission 2*, p. 6.

144 Law Institute of Victoria, *Submission 36*, p. 7.