

Chapter 6

Australian Privacy Principle 3—collection of solicited personal information

Introduction

6.1 Australian Privacy Principle 3 (APP 3) deals with the collection of solicited personal information including sensitive information. The Companion Guide notes that personal information should only be collected where it is necessary for, or directly related to, one or more of the entity's functions or activities (the functions test). It also provides that an entity must collect information directly from an individual unless it is unreasonable, or impracticable, to do so. If the personal information is sensitive information, the individual must also consent to the collection.¹

6.2 However, APP 3 provides for a number of exemptions on public interest grounds. These exemptions included exemptions based on National Privacy Principle 10.1 and a number of new provisions. The new provisions reflect the application of this principle to both agencies and organisations.

Background

6.3 Information Privacy Principles (IPPs) 1–3 cover the collection of personal information by agencies. Personal information is not to be collected by agencies unless the purpose is lawful and directly related to the functions or activities of the collector and the collection is necessary. Agencies are to take reasonable steps to ensure that the individual is aware of, among other things, the purpose for which the information is collected and that the information collected is relevant, up-to-date and complete and the collection does not intrude unreasonably on the individual's personal affairs.² The IPPs do not regulate the collection of sensitive information separately from other forms of personal information.

6.4 National Privacy Principles (NPPs) provide that an organisation may only collect personal information that is necessary for its functions or activities; and by lawful and fair means. Organisations are to take reasonable steps to ensure that the individual is aware of certain matters including that he or she can access the information. In addition, the collection may be from the individual, if it is reasonable and practicable to do so, or from someone else if reasonable steps are taken to ensure that the individual is aware of certain matters except in the case where making the

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

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 710–11.

individual aware would pose a serious threat to anyone's life or health.³ In relation to sensitive information, the NPPs prohibit the collection of sensitive information except in certain circumstances including that the individual has consented and the collection is required by law. In addition, non-profit organisations are permitted to collect sensitive personal information in certain circumstances.⁴

6.5 The ALRC noted that neither the IPPs nor NPPs require that an individual give his or her consent before an agency or organisation is permitted to collect the individual's personal information.

6.6 The ALRC's review canvassed the issue of collection of personal information directly from an individual, where reasonable and practicable to do so. The ALRC concluded that both agencies and organisations should only collect information from the individual to whom the information relates, where it is reasonable and practicable to do so, and noted that 'such a requirement will increase the likelihood that personal information collected will be accurate, relevant, complete and up-to-date. It also gives individuals an opportunity to participate in the collection process'.⁵ The ALRC was of the view that the 'reasonable and practicable' requirement would not limit the coercive information gathering powers of agencies or the exercise of their intelligence, investigative and compliance functions. However, the ALRC recommended that the Office of the Privacy Commissioner (OPC) develop and publish guidance to clarify when it would not be reasonable or practicable to collect personal information only from the individual concerned.⁶

6.7 The ALRC's consideration of the collection of sensitive personal information focused on whether agencies should also be subject to restrictions in collecting sensitive information. The ALRC concluded that there were strong policy reasons to extend restrictions on collection of sensitive information to agencies and noted:

The risks associated with sensitive information being subsequently misused are sufficiently serious to justify imposing an obligation on agencies to abide by restrictions on the collection of sensitive information. Such restrictions however, should allow for the collection of sensitive information by agencies for legitimate reasons.⁷

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 711.

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 735–36.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 718.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 718–19.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 740–41.

6.8 In addition, the ALRC saw no reason for a separate privacy principle to deal with the collection of sensitive information. Rather, it recommended a single principle dealing with the collection of all personal information.⁸

6.9 There are a range of exceptions to the prohibition against the collection of sensitive personal information. The ALRC commented as follows:

- *required or authorised by or under law*: the ALRC concluded that an exception where the collection of sensitive information is required by law is too narrow; rather, the legitimate collection of sensitive information authorised by law should be included in the principle. Concerns that 'specific' authorisation to collect sensitive information is rarely provided for in legislation were acknowledged in the review and it was noted that a review of current legislation may be required to ensure that, where needed, the collection of sensitive information is specifically authorised;⁹ and
- *emergency situations*: in emergency situations, where an individual is unable to give consent, the ALRC noted that the Privacy Act contains a separate regime for the collection, use and disclosure of personal information in situations where the Prime Minister or a minister has declared an emergency or disaster. In addition, NPP 10 generally allows for the collection of sensitive information by organisations where it is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual and the individual is incapable of giving consent. The ALRC considered the application of NPP 10 to both agencies and organisations and concluded that it should apply to agencies. However, the ALRC did not support the current requirement of NPP 10 that the threat must be both serious and imminent as it saw this as too difficult to satisfy. The ALRC was of the view that the wording should be relaxed so that it is triggered where the threat is serious, but not necessarily imminent.¹⁰

6.10 The ALRC also considered other circumstances where exceptions may be warranted; for example, collecting sensitive personal information where essential services are to be provided to individuals incapable of giving consent. The ALRC did not consider that the benefits would outweigh the difficulties of the creation and implementation of such an exception.¹¹

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 741.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 738–41.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 741–44.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 748–751.

6.11 In relation to the other exceptions currently contained in NPP 10.1, the ALRC commented:

- *consent exception:* NPP 10 allows for sensitive personal information to be collected where the individual has given consent. The ALRC concluded that it is undesirable to amend the consent exception to require express consent for the collection of sensitive information;
- *exception relating to non-profit organisations:* non-profit organisations may collect information in the course of their activities where certain specified conditions are met. The ALRC commented that concerns about the drafting of this exception are best addressed by the Office of the Parliamentary Counsel;
- *exception relating to legal and equitable claims:* collection is permitted where it is necessary for the establishment of, exercise or defence of, a legal or equitable claim. The ALRC was not convinced that there was a need to broaden this exception but did not receive sufficient feedback from stakeholders to make a proper assessment of the merits of broadening the exception. The ALRC did not recommend an amendment to this exception; and
- *exception relating to alternative dispute resolution:* the ALRC was of the view that collecting sensitive information should be permitted where it is necessary for the purpose of confidential alternative dispute resolution.¹²

Government response

6.12 The Government accepted in full all but one of the ALRC's recommendations in relation to collection of sensitive information. The Government accepted in part the ALRC's recommendation that the sensitive information provisions should contain an exception permitting the collection of sensitive information by an entity where it is necessary to lessen or prevent a serious threat to life or health or the individual is legally or physically incapable of giving or communicating consent. The Government response noted that for consistency, a 'serious threat' should refer to 'life, health or safety'.¹³

Issues

6.13 Some submitters expressed their supported for APP 3.¹⁴ However, Professor Graham Greenleaf and Mr Nigel Waters argued that APP 3 is 'significantly weaker

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 752–55.

13 Australian Government, *Enhancing National Privacy Protection: Australian Government First Stage Response to the Australian Law Reform Commission Report 108, For Your Information: Australian Privacy Law and Practice*, October 2009, p. 44.

14 Office of the Guardian for Children and Young People, *Submission 4*, p. 4; Australian Bankers' Association, *Submission 15*, p. 4; Office of the Health Services Commissioner, *Submission 26*, p. 2.

than the equivalent NPP(1)' and pointed to a number of concerns including the use of the term 'reasonably necessary' rather than 'necessary'.¹⁵ The matters raised by Professor Greenleaf and Mr Waters and other submitters are addressed below.

Structure

6.14 The committee received a range of comments relating to the structure of APP 3. While welcoming the concept of distinguishing between the collection of solicited and collection of unsolicited information, the Australian Institute of Credit Management (AICM) was of the view that the collection of sensitive information should also be placed in a separate principle. The AICM commented that entities did not always recognise information that is necessary to the entity's functions as being 'sensitive information' and that it should be managed with considerable care.¹⁶

6.15 The OPC also commented on a number of matters related to the structure of APP 3. First, the OPC was of the view that the principle should be titled 'Collection of personal information' and secondly, that the collection of unsolicited information be incorporated into the principle. This latter matter is considered by the committee in chapter 7.

6.16 Secondly, the OPC suggested that APP 3 could be simplified by removing matters which it considered to be repetitious and redundant (APP 3(2)(a)(i)) and consolidating the exceptions as a simpler list under APP 3(2). This would reflect the structure of NPP 10 and the ALRC's model Unified Privacy Principles.¹⁷ Similarly, Professor Greenleaf and Mr Waters suggested consolidation of APP 3(2) and APP 3(3) to simplify the principle.¹⁸

6.17 Privacy NSW commented that the complex wording of APP 3 'defeats the purpose in choosing principle-based rules rather than legislation' and argued for a more simply expressed principle.¹⁹ Qantas also argued that APP 3 contained 'unnecessary verbiage' with APP 3(2)(a)(i) merely repeating the provisions contained in APP 3(1) while APP 3(5) (third person collection), which replicates NPP 1.4, does so in a less clear and more verbose way.²⁰

15 Professor G Greenleaf and Mr N Waters, *Submission 25*, p. 6; see also Australian Privacy Foundation, *Submission 33*, p. 2.

16 Australian Institute of Credit Management, *Submission 8*, p. 2.

17 Office of the Privacy Commissioner, *Submission 39*, p. 27.

18 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

19 Privacy NSW, *Submission 29*, p. 3.

20 Qantas, *Submission 38*, p. 5.

Conclusion

6.18 In chapter 3, the committee has commented on the need to refine the APPs. The committee considers that APP 3 is another example of where simplifying the approach taken would improve the readability of the principle.

Use of the term 'reasonably necessary for, or directly related to'

6.19 The committee received a range of comments in relation to the use of the term 'reasonably necessary for, or directly related to' in APP 3. The AFC supported the inclusion of the term 'reasonably' necessary as reflecting a 'compliance framework that appropriately balances privacy and public interest rights'. However, the AFC did not support the addition of the 'directly' to the 'related to' element as it was argued that this did not appear to be in line with the recommendations of the ALRC. Such wording, it was argued, adds an 'unnecessarily prescriptive aspect to this component of the principle and is at odds with the Government's high-level, non-prescriptive approach and an appropriate balance between the interests of the individual and the public'.²¹

6.20 Other submitters, including Professor Greenleaf and Mr Waters, commented that the proposed wording of APP 3 would result in weaker privacy protections as it was argued that the 'reasonably necessary' test broadened the principle.²² The Victorian Privacy Commissioner voiced concern about the use of both the terms 'reasonably necessary' and 'directly related to' and commented on the need to ensure that protections were not lowered:

The APPs should represent the highest standard of privacy protection currently enjoyed in Australia, not the lowest common denominator. Agencies or organisations should only collect personal information that is *necessary* for their functions or activities (as provided by the current VIPP 1.1 in the Information Privacy Act), not information that an agency or organisation reasonably believes may be necessary for their functions or activities, or which is directly related to them.²³

6.21 One of the weaknesses, it was argued, arises as APP 3(1) 'allows multi-function entities to request personal information that is not directly related to the goods or services actually requested by the individual' as the information may be reasonably necessary for any one of the entity's functions.²⁴ Dr Colin Bennett was of the same view that the use of 'reasonably necessary' allowed entities to state a very broad set of goals and purposes and thereby allows for any collection of personal

21 Australian Finance Conference, *Submission 12*, p. 4.

22 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 6–7.

23 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 4.

24 Law Institute of Victoria, *Submission 36*, p. 5.

information to be 'reasonably necessary' or 'directly related to' their functions and activities.²⁵

6.22 Both the LIV and Dr Bennett noted that the Companion Guide indicates that 'reasonably necessary' means that 'from the perspective of a reasonable person the function or activity is legitimate for that type of entity', and is intended to be interpreted objectively and in a practical way. However, Dr Bennett argued that the proposed drafting of APP 3 does not make this clear.²⁶ The LIV stated APP 3 focuses only on the entity's functions and not on the individual's reasons for disclosing personal information or dealing with the entity.²⁷ Professor Greenleaf and Mr Waters also commented that the test should be 'the reasonableness of the purpose' rather than merely the reasonableness of information collection in the context of the entity's functions or activities.²⁸

6.23 The LIV recommended that the wording be amended to include 'reasonably necessary for the function or activity in which the person is engaging'.²⁹ Professor Greenleaf and Mr Waters suggested that 'necessary' alone or preferably 'necessary and directly related to' the entity's functions or activities would strengthen APP 3.³⁰

6.24 The OPC noted that the Government had accepted the ALRC's recommendation on 'collection' and it had stated that 'necessary' should be interpreted objectively and in a practical sense.³¹ The OPC considered that, in line with the Government response, and the ALRC's recommendation, the phrase 'necessary for one or more of the entity's functions or activities' was sufficient for all entities under a single set of principles. However, APP 3 includes the 'directly related to' alternative. The OPC argued that this is unnecessary for agencies as often agency functions and activities are tied to enabling legislation, object clauses or related instruments and are thus more easily defined. The OPC concluded that it was not aware of examples where the 'necessary' requirement would prevent an agency from collecting personal information to pursue legitimate functions or activities.

6.25 In relation to organisations, the OPC was of the view that the wording of APP 3 appears to lower the existing NPP standard for organisations, including when collecting sensitive information. The OPC was concerned that uncertainty had been introduced and that this would allow a broader range of personal information to be collected, including sensitive personal information. The OPC concluded that this 'could be inconsistent with the intent of enhanced, not diminished, privacy protections'

25 Dr Colin Bennett, *Submission 11*, p. 2.

26 Dr Colin Bennett, *Submission 11*, p. 2.

27 Law Institute of Victoria, *Submission 36*, p. 5.

28 Professor G Greenleaf & Mr N Waters, *Submission 25*, pp 6–7.

29 Law Institute of Victoria, *Submission 36*, p. 5.

30 See also Dr Colin Bennett, *Submission 11*, p. 2.

31 Government Response, p. 42.

and recommended that, to maintain the current level of protection in NPP 1, the words 'or directly related to' be removed from APP 3(1) and corresponding provisions.³²

6.26 Privacy Law Consulting provided a further view in relation to the interpretation of APP 3 contained in the Companion Guide.³³ Privacy Law Consulting suggested that the interpretation provided does not appear to be consistent with the literal reading of APP 3 and continued:

The interpretation referred to in the Companion Guide would result in the Privacy Act effectively regulating, and limiting, the types of functions and activities an entity could perform or engage in (based on a test relating to whether they were reasonably legitimate for that type of entity). Such an outcome appears to be beyond the intended scope and purpose of the Act. Further, this would be inconsistent with the general demise of the doctrine of ultra vires in respect of corporations (which placed limitations on activities a corporation could engage in based on its objects clause in its memorandum of association) – see, for example, s 124(1) of the *Corporations Act 2001* (Cth) which generally provides that companies have the legal capacity and powers of an individual, effectively abolishing the application of the doctrine in relation to corporations established under that Act.

It is important that any uncertainty in this regard be eliminated, otherwise entities operate under the spectre that functions or activities they perform or engage in could be challenged on privacy grounds.³⁴

6.27 At the committee's hearing on the exposure draft, Professor Rosalind Croucher, President, ALRC was asked to respond to concerns about the possible weakening of the collection principle under proposed APP 3.³⁵ In a written response, Professor Croucher stated that the UPP recommended by the ALRC followed NPP 1.1 rather than IPP 1.1 as the ALRC was of the view that the NPPs should form the general template for the drafting and structuring of the new unified principles.

6.28 Professor Croucher went on to state that 'it is not entirely clear whether the formulation in APP 3(1) provides more or less privacy protection than that in NPP 1.1' and commented:

Arguably, allowing the collection of information where it is "directly related" to a function or activity, as well as where it is "necessary", broadens the scope for collection. However, as discussed in ALRC Report 108, the Office of the Privacy Commissioner's 2001 guidelines on collection of information by organisations provide that:

32 Office of the Privacy Commissioner, *Submission 39*, p. 26.

33 Privacy Law Consulting, *Submission 24*, p. 2.

34 Privacy Law Consulting, *Submission 24*, p. 2.

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

The Commissioner interprets "necessary" in a practical sense. If an organisation cannot in practice effectively pursue a legitimate function or activity without collecting personal information, then the Commissioner would ordinarily consider it necessary for that function or activity. (p 27)

Further, the High Court of Australia has noted that there is a long history of judicial and legislative use of the term 'necessary', not as meaning 'essential or indispensable', but as meaning 'reasonably appropriate and adapted' (see *Mulholland v Australian Electoral Commission* (2004) 220 CLR 181, [39]).

It should also be observed that, arguably, APP 3 is more privacy protective than NPP 1 in that it requires that collection is 'reasonably' necessary. The addition of this objective element was an option considered, but rejected as unnecessary, in ALRC Report 108, [21.77].³⁶

6.29 The Department of the Prime Minister and Cabinet (the department) also provided answers to questions on notice in relation to APP 3. The department commented that the wording in APP 3(1) is intended to strike the appropriate balance between the need to protect against the unnecessary collection of personal information and the need for organisations and agencies to collect personal information reasonably necessary for, or directly related to, one or more of the their functions or activities.

6.30 The department explained the basis of APP 3 as follows. There are two key elements to APP 3(1): first, a 'reasonably necessary' test is included in relation to the collection of 'personal information other than sensitive information'. This is consistent with the views of the ALRC that an objective test should continue to apply as is currently the case for organisations under NPP 1 (although the ALRC believed that an objective test was implied even with the use of only 'necessary'). The department argued that the requirement on entities to collect only personal information that is reasonably necessary to their functions, requires the collection of personal information to be justifiable on objective grounds, rather than on the subjective views of the entity itself. The department concluded that this will limit inappropriate collection by entities.

6.31 Secondly, the term 'directly related to' one or more of the entity's functions or activities ensures that there must be a clear connection between the collection and the entity's functions or activities. The department commented that that aspect of the test appears in the existing IPPs, which bind agencies. The department also noted that IPP 1 has operated under the existing regime in circumstances where it may not be possible to meet the 'reasonably necessary' test. This element is being retained because there may be agencies (less so for organisations) that need to collect personal information to effectively carry out defined functions or activities but who may not meet an objective 'reasonably necessary' test.³⁷

36 Australian Law Reform Commission, *Answers to Question on Notice*, pp 1–2.

37 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 9.

Conclusion

6.32 The committee agrees that an objective test is a necessary element in the collection principle. However, given the comments in relation to the addition of the word 'reasonably' in the 'necessary' test, the committee remains to be persuaded that this provides a higher, or even the same, level of privacy protection as the wording of NPP 1.

6.33 In relation to the 'directly related to' test, the committee notes the department's comments that this test appears in the IPPs as there are circumstances where an agency may not meet the 'reasonably necessary' test. The department goes on to comment that this is less of an occurrence for organisations. The committee has taken note of the comments in relation to the potential for organisations to use this test to establish a very broad set of activities and functions on which to base the collection of personal information and at the same time comply with APP 3.

6.34 The committee considers that APP 3 is a less than elegant solution to the drafting of a unified collection principle, and may, in effect, lower privacy protections by allowing organisations to take advantage of a provision which is more appropriately applied to agencies. The committee considers that the 'reasonably necessary' test provides organisations with sufficient flexibility, and is, in fact, substantially similar to what is now provided in NPP 1. The committee therefore does not support the extension of the 'directly related to' test to organisations and recommends that APP 3 should be reconsidered.

Recommendation 8

6.35 The committee recommends that in relation to the collection of solicited information principle (APP 3), further consideration be given to:

- **whether the addition of the word 'reasonably' in the 'necessary' test weakens the principle; and**
- **excluding organisations from the application of the 'directly related to' test to ensure that privacy protections are not compromised.**

Consent

6.36 The committee received comments regarding the consent requirements of APP 3 in relation to sensitive information. APP 3(2) requires that an entity must not collect sensitive information unless the individual consents or the collection falls within an exception listed in APP 3(3). The general issue of consent has been discussed in chapter 3.

Sensitive information

6.37 Generally, the collection of sensitive information should not occur unless the collection meets the functions test and the individual has consented (APP 3(2)). However, there are a number of specific exemptions which allow collection of sensitive information without consent (APP 3(3)).

6.38 The OPC's comments in relation to the collection of sensitive information went to the use of the 'directly related to' test. The OPC was of the opinion that collecting sensitive information should be 'necessary' not 'directly related to' the functions or activities of an agency or organisation. The OPC commented that the drafting of APP 3(2) 'appears to mean that if an exception in APP 3(3) applies, sensitive information may be collected even if it is not 'reasonably necessary for' or 'directly related to' the entity's functions or activities'. As a consequence, APP 3 provides for a lower threshold for the collection of sensitive personal information than does the existing NPP 1. The OPC concluded:

If the collection of sensitive information is not subject to the same basic test of "necessity" as other personal information in APP 3(1), this is inconsistent with the accepted view that sensitive information should be accorded higher protection.³⁸

6.39 The department agreed with the OPC's interpretation that 'sensitive information' could be acquired using an exception in APP 3(3) without the information first needing to be 'reasonably necessary' or 'directly related to' an activity or function of the entity. However, the department pointed out that these exceptions are based on circumstances where there is an overriding public interest in collecting the information and that safeguards have been built into most of the exceptions. The department stated that the safeguards will ensure that, even where there are specific special circumstances, there is still a requirement that collection be based on an objective element (either relating to reasonable necessity or reasonable belief of necessity).³⁹

6.40 Submitters also provided a range views on the individual exceptions provided for in APP 3(3). Professor Greenleaf and Mr Waters, for example, argued that the exceptions had been 'dramatically expanded' citing in particular the 'required by law' and 'emergencies' exceptions.⁴⁰ Other submitters provided comment on specific exceptions.

Required or authorised by or under Australian law

6.41 APP 3(3)(a) provides an exception in the case of the collection of sensitive personal information that 'is required or authorised by or under an Australian law, or an order of a court or tribunal'. The Victorian Privacy Commissioner voiced concern about this exception, noting that it is similar, but not as stringent, as that contained in the Victorian privacy legislation. The Commissioner stated that the APPs should represent the highest level of current privacy protection in Australia. The Commissioner supported a narrower drafting of the requirement so that an exception

38 Office of the Privacy Commissioner, *Submission 39*, p. 27.

39 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 10.

40 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

is only permissible when the requirement to collect sensitive information is mandatory, and not simply permissive or discretionary.⁴¹

6.42 Professor Greenleaf and Mr Waters commented that no justification had been provided as to why the 'deliberately more protective wording' of NPP 10 has been abandoned. While accepting that "specifically authorised" may be an appropriate change to this requirement, they did not support 'the wholesale invocation of the very vague and subjective "authorised"'.⁴²

Emergencies

6.43 An exception is provided for when an entity believes the collection is necessary to 'lessen or prevent a serious threat to the life, health or safety of any individual or to public health or safety' and it is unreasonable or impracticable to obtain the consent of the affected person (APP 3(3)(b)).

6.44 This exception was criticised by Professor Greenleaf and Mr Waters as it was argued that it had been broadened by the removal of the 'imminent' threat criteria. They submitted that it is 'essential to retain a test of "urgency" to justify why another basis for [collection] cannot be established'. In addition, they stated that the exception has also been broadened by the addition of threats to an individual's 'safety' and to 'public health or safety' and by the replacement of the condition that consent be physically or legally impracticable with a much weaker 'unreasonable or impracticable to obtain consent'. Professor Greenleaf and Mr Waters commented that the last change 'is a major weakening of the principle and will be interpreted by entities to routinely justify collection of sensitive information without consent'.⁴³

6.45 The Public Interest Advocacy Centre (PIAC) also commented on the absence of the requirement that the threat be 'imminent'. PIAC argued that there must be some degree of urgency and, as a result of that urgency, limited access to other mechanisms available to prevent the threat eventuating. PIAC was of the view that the requirement of imminence acted as an important safeguard, particularly when information was being sought about persons with mental illness. In this case, there may be a potential for serious threat to health, but no imminence, because at the relevant time the illness is well controlled by medication or is episodic and the person is currently not unwell. PIAC concluded that where the threat is serious, but not imminent, other mechanisms should be used to avoid the threat eventuating without recourse to non-consensual collection of sensitive information.⁴⁴

6.46 Qantas, however, argued that the reference to 'serious' should be removed as the question of seriousness is subjective and it 'believed that employees should not be

41 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 5.

42 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

43 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

44 Public Interest Advocacy Centre, *Submission 32, Attachment 1*, p. 8.

placed in the position of having to make such a judgment if they reasonably believe that a serious threat exists and it will be unreasonable and impractical to obtain consent'.⁴⁵

6.47 The department provided the following information in relation to the emergencies exception. The ALRC Report stated that the current requirement that a threat must be both serious and imminent in these provisions is too difficult to satisfy, sets a 'disproportionately high bar' and can lead to personal information not being used or disclosed in circumstances where there are compelling reasons justifying its use or disclosure. The removal of 'imminent' would also allow an agency or organisation to take preventative action to stop a threat from developing into a crisis.

6.48 The ALRC's view was accepted by the Government. The department noted that, to address concerns of a number of stakeholders that the removal of this element would inappropriately broaden the exception, a requirement was included that use and disclosure could occur only after consent has first been sought, where to do so is reasonable and practicable. Thus, the additional elements to the exception where 'it is unreasonable or impracticable to obtain the affected individual's consent' to either the collection of sensitive information, or the use or disclosure of personal information.⁴⁶

Unlawful activity

6.49 It was noted that the exception relating to the investigation of unlawful activity was not included in the ALRC's recommendations. Professor Greenleaf and Mr Waters commented that there needs to be some justification for this exception and that it should be qualified on the condition that the entity must take some appropriate action within a reasonable period of time. It was argued that 'without such a condition, the exception invites the compilation and indefinite maintenance of "blacklists" based on suspicion of wrongdoing but without any requirement for individuals on such lists to be afforded natural justice'.⁴⁷

Missing persons

6.50 An exception (APP 3(3)(g)) is available to assist in the location of missing persons. Collection of the information must comply with the Australian Privacy Rules. Professor Greenleaf and Mr Waters argued that, if there is a case for a separate exception for missing persons, the provisions should be contained in the APP and not in the, as yet unknown, Australian Privacy Rule.⁴⁸

6.51 The ALRC did not support the creation of an express exception for disclosing information to assist in missing persons investigations as other exceptions would

45 Qantas, *Submission 38*, pp 4–5.

46 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 10.

47 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

48 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 8.

assist in broadening the scope of situations in which disclosure of personal information in missing persons investigations would be authorised, such as the serious threat exception. The department noted that the Government agreed with the ALRC's view that using or disclosing personal information to locate missing persons may often be permitted by other exceptions. However, the Government considered that 'an express exception should also apply for those instances where the application of other exceptions is unclear'. For example, some agencies were concerned that the 'serious threat to life' etc exception would not allow them to collect information relating to a missing person who may have gone missing because of health issues. The department went on to state that, in order to provide safeguards against improper use of such information, the Government decided that such collection, uses or disclosures should be in accordance with binding rules issued by the Australian Information Commissioner. These are to be in the form of a legislative instrument and therefore subject to the scrutiny of Parliament.⁴⁹

6.52 The department provided further information about the rules and commented that they will consist of detailed matters relating to the procedures and protocols used by agencies that are more appropriately dealt with in subordinate legislation. The department noted that using rules, rather than the Act, will allow a more flexible response to the wide variety of circumstances in which this issue may arise (e.g. natural disasters, child abductions). Further, there is already an example of a non-legislative determination (Public Interest Determination 7) where the Privacy Commissioner has granted a waiver from compliance with IPP 11.1 which permits the Department of Foreign Affairs and Trade to disclose personal information of Australians overseas to their next of kin in certain limited circumstances. The rules will also be subject to extensive consultation and to parliamentary scrutiny.

6.53 The department noted that the Government response provides a non-exhaustive list of matters which may be included in the rules.⁵⁰

Exceptions related to Commonwealth agencies

6.54 There are a number of exceptions (APP 3(3)(e) and (f)) which apply only to Commonwealth agencies; for example, the Defence Force. The Victorian Privacy Commissioner commented that this was problematic when expressly included in the APP itself, as this reduces the simplicity, lucidity and 'high-level' nature of the APPs. In addition, the Commissioner stated that it would reduce the ability of states and territories to readily adopt them with minimal amendment.⁵¹

6.55 Professor Greenleaf and Mr Waters saw these special exceptions as allowing the Defence Forces and diplomatic service 'to avoid the principle [on] the basis of their own "reasonable belief".' They argued that this reflected 'a lazy approach to

49 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 11.

50 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 12.

51 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 5.

compliance' and that these entities should have to comply with APP 3 and take advantage of the generic exceptions where appropriate.⁵²

6.56 The OPC's comments on the inclusion of agency specific exceptions in the APPs are provided in chapter 3.

Implied consent

6.57 Qantas submitted that it often collected sensitive personal information provided by a third party where it is impracticable to obtain consent from the individual about whom it is given; for example, in the case of a carer providing health information while making a booking for the person in their care. Qantas submitted that in these circumstances the consent exception should be expanded to include the situation where consent can be reasonably be inferred from the circumstances of the collection.⁵³

Health information

6.58 The NSW Department of Justice and Attorney General raised the concern that APP 3 did not allow for the collection of sensitive health information such as where in providing care for a patient, a family history is taken. It was argued that a health practitioner will not have the patient's family member's consent and in most circumstances, the information collected about the patient's family members will not be necessary to lessen or prevent a serious threat to life, health or safety. The NSW Department of Justice and Attorney General concluded:

It is imperative that health practitioners can continue to take a patient's family history without having to seek the consent of each family member to collect health information about that family member. APP3 should be amended to allow this to occur.⁵⁴

Conclusion

6.59 The committee notes that the exceptions provided for in APP 3 are 'based on circumstances where there is an overriding public interest in collecting information'. To ensure that these provisions are not abused, safeguards have been incorporated into the exceptions. In particular the committee notes that, in relation to the missing persons exception, Australian Privacy Rules will provide for detailed matters relating to procedures and protocols. The committee considers that this is an appropriate exception to deal with the sometimes very difficult circumstances of missing persons. The use of rules, rather than a non-legislative determination by the Privacy Commissioner, provides for consultation and the scrutiny of Parliament. The committee welcomes this approach.

52 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 7.

53 Qantas, *Submission 38*, p. 5.

54 NSW Department of Justice and Attorney General, *Submission 42*, p. 5.

6.60 In relation to the inclusion of agency specific exceptions, the committee has commented on this matter in chapter 3.

Means of collection

6.61 APP 3(5) provides that entities must collect information only by lawful and fair means and the entity must collect the information from the individual concerned. Two exceptions are provided for. The first, APP 3(5)(a), allows agencies to collect information about a person from a third party if required or authorised by or under an Australian law, or by a court or tribunal. The second, APP 3(5)(b), applies where it is 'unreasonable or impracticable' for an entity to collect the information from the individual.

6.62 The Victorian Privacy Commissioner strongly supported the provisions in relation to the direct collection of information from an individual and noted that it enables individuals to have some measure of control over what is collected, by whom and for what purposes as well as allowing individuals to refuse to participate in the collection.⁵⁵ The inclusion of the 'reasonable and practicable' requirement was also supported by the Victorian Privacy Commissioner as it allows for circumstances where it may not be practically possible to collect information directly from an individual. However, the Commissioner and the LIV saw the need for guidance as to the circumstances where it would not be reasonable or practicable to collect information directly from an individual. This should be jointly prepared by all Privacy (or Information) Commissioners across jurisdictions.⁵⁶

6.63 The LIV also noted that APP 3(5)(b) does not expressly restrict an entity from on-selling to a third party entity personal information obtained from an individual if it is 'unreasonable or impracticable' for the third party to collect the information from an individual. For example, the third party entity may mount an argument that it was 'unreasonable or impracticable' to collect the information from the individual because of lack of time. The LIV expressed concern that individuals may not have control over where information about them goes, or is used, and recommended guidance on the circumstances in which collection from an individual is deemed to be 'unreasonable or impracticable'.⁵⁷

Collection from third parties

6.64 The restriction to agencies of the collection of information from a third party, if required or authorised by or under an Australian law, was questioned by the ACF. It commented that it 'was not aware of any policy justification for confining the permitted means to collection to include third parties to the public sector' and that this

55 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 5.

56 Office of the Privacy Commissioner Victoria, *Submission 5*, p. 6.

57 Law Institute of Victoria, *Submission 36*, p. 5.

could equally be relevant to the private sector.⁵⁸ The Australian Bankers' Association also supported this recommendation as there is increased use of third party verification methods to satisfy legislative requirements, such as anti-money laundering and counter terrorism legislation as well as instances where a third party is required to translate for non-English speaking customers. The ABA recommended that the APP be amended to allow for sensitive information to be collected from a third party where consent has been given.⁵⁹

6.65 The NSW Department of Justice and Attorney General also commented on the collection of information from third persons. It pointed to the NSW Law Reform Commission's recommendation that an entity should be able to collect personal information about an individual from a third person if the individual consents. The basis of this recommendation was that it gives autonomy to the individual about how their personal information may be collected; for example, the person may find it more convenient to allow the information to be collected from a third party. In addition, the NSW Department of Justice and Attorney General pointed to the circumstances facing some agencies. For example, the NSW Department of Housing may need to collect information from a medical practitioner about the mental health of an applicant for priority housing. It is possible that in such a case, it might not be unreasonable or impracticable to obtain the information from the individual in question. Thus, as presently drafted, APP 3 might not authorise the Department to obtain such information from the medical practitioner.

6.66 The NSW Department of Justice and Attorney General noted the comments of the ALRC in relation to this matter: that if personal information is collected from a third person with their consent, individuals will not have the opportunity to refuse to provide information and there is a risk that third parties will not be able to provide up-to-date, complete or accurate information. However, the NSW Department of Justice and Attorney General commented that if a 'consent' exception was considered, it may be appropriate that it relied on 'express' consent. It was concluded that:

While there are some risks in relation to the nature of the consent and the accuracy and completeness of the information, individuals should be free to choose to have their information collected from third parties where they do not wish to provide the information themselves.⁶⁰

6.67 The department responded to issues raised in relation to 'means of collection', in particular, collection from third parties. The department commented that the exception in APP3(5)(a) was included to address agency concerns that they may be in breach of the Privacy Act where another law allows or requires them to collect from a number of sources other than the individual, but in the circumstances it would still be practicable and reasonable to go to the individual. For example, the Australian

58 Australian Finance Conference, *Submission 12*, p. 4.

59 Australian Bankers' Association, *Submission 15*, p. 4.

60 NSW Department of Justice and Attorney General, *Submission 42*, p. 5.

Electoral Commission obtains information from Commonwealth agencies and updates the electoral roll using that information.⁶¹

6.68 The department went on to explain that currently, NPP 1 allows organisations, where reasonable and practicable, to collect personal information about an individual *only* from that individual. The ALRC did not recommend any change to this. In relation to the concerns raised by the ABA, the department commented that when an entity collects information from a third party for identity verification purposes in accordance with legislative requirements under anti-money laundering and counter terrorism legislation, because it had a suspicion that the person is not who they claim to be, it is likely to be "unreasonable or impracticable" to collect it from the individual concerned. The department concluded that the alternative second element of the exception would apply to allow the collection.⁶²

Conclusion

6.69 The committee is of the view that the inclusion of the 'unreasonable and impractical' provision in APP 3(5)(b) provides appropriate flexibility to organisations and therefore there is no need to extend APP 3(5)(a) to organisations.

6.70 The committee has noted the comments of The NSW Department of Justice and Attorney General in relation to the collection of personal information about an individual from a third party when that individual consents to that process. The committee considers that, at the present time, it appears that the risks to privacy outweigh potential benefits.

61 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 12.

62 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, pp 12–13.