Chapter 4

Australian Privacy Principle 1–open and transparent management of personal information

Introduction

4.1 Australian Privacy Principle 1 (APP 1) addresses open and transparent management of personal information. The Companion Guide states that the requirement for open and transparent management is the first APP because 'it will emphasise that entities should first plan ***how*** they will handle personal information before they collect and process it'. In addition, it will make sure that entities consider their privacy obligations when planning new systems. The Companion Guide noted that this reflects international moves towards a 'privacy by design' approach, so that information systems include privacy and data protection compliance from their inception.[1]

Background

4.2 In its review, the Australian Law Reform Commission (ALRC) considered the openness requirements of the privacy regime. The ALRC concluded that there should be a discrete principle requiring an agency or organisation to operate openly and transparently by providing general information on how it manages personal information. It was noted that compliance with openness requirements generally benefits the regulatory system as a whole and 'therefore, plays a key role in promoting best practice in the handling of personal information'.[2] In addition, the development and publication of privacy policies will promote accountability and increase the transparency of the information handling practices of entities.

4.3 Although both the Information Privacy Principles (IPPs) and the National Privacy Principles (NPPs) set out openness requirements, openness is achieved by different regulatory mechanisms for agencies and organisations. The ALRC was of the view that there should be one consolidated and simplified openness requirement and stated:

> The 'Openness' principle should make it clear that a Privacy Policy is the regulatory mechanism by which agencies and organisations are to achieve openness. Agencies and organisations should be required to set out in Privacy Policies clearly expressed policies on their handling of personal information.[3]

---

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

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 810.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* ALRC 108, 2008, p. 812.

4.4 The ALRC also considered the content of a privacy policy. While the NPPs impose a general obligation to maintain a privacy policy document, the IPPs take a more prescriptive approach and list specific matters to be included in the record summarising how an agency handles personal information.[4] The ALRC concluded that the essential content of a privacy policy should be expressed in high-level terms. The ALRC was of the view that 'the central obligation should be for agencies and organisations to set out in such a document clearly expressed policies on an agency's or organisation's handling of personal information, including how it collects, holds, uses and discloses personal information'. In addition, any matters required in a privacy policy should not be regarded as being exhaustive.[5]

4.5 The ALRC considered specific matters to be included in a privacy policy and recommended that the list of matters should be limited, but include the sort of personal information held, and the purpose for which that information is held. Other matters required in a privacy policy included the steps available to an individual to access and correct personal information and avenues for complaint.[6]

4.6 The mechanisms for making privacy policies available were canvassed in the review, with the ALRC commenting that loading policies onto websites was 'an ideal mechanism for making them generally available'. In addition, the ALRC recommended that hard copies should be made available on request or in a form accessible for those with special needs.[7]

4.7 The development of short form privacy notices was also examined. The ALRC concluded that short form privacy notices serve a useful purpose and recommended that the Office of the Privacy Commissioner (OPC) should continue to encourage and assist entities to make these available.[8]

Government response

4.8 The Government accepted the ALRC's recommendations in relation to the availability of privacy policies and the development of short form privacy notices and accepted, with amendments, the ALRC's main recommendation in relation to a single openness principle and the matters to be included in a privacy policy.

---

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 813.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 819.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 821–22.

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 822–25.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 825–29.

4.9 The Government response stated:

> The Government agrees that organisations and agencies should consider their personal information handling policies and practices and clearly set these out in a Privacy Policy available to all individuals. This helps to promote transparency in the handling of personal information, as well as consumer control, choice and trust in how their information will be handled.
>
> The Government also agrees that requiring agencies and organisations to express in their Privacy Policies how they handle personal information at each stage of the information cycle, will encourage them to consider how the Privacy Principles apply to their activities.[9]

4.10 The Government outlined the areas where it intended to make amendments to the ALRC's recommendation as follows:

- in order to align the Privacy Principles with the stages of the information handling cycle, the 'openness' principle is to be the first enumerated privacy principle;
- in addition to the obligations proposed by the ALRC, the 'openness' principle should also require entities to take reasonable steps, having regard to the circumstances of the agency or organisation, to develop and implement internal policies and practices that enable compliances with the Privacy Principles including staff training;
- a general obligation to take reasonable steps to implement policies and practices that ensure compliance with the Privacy Principles is to be included in the openness principle in order to ensure a proactive approach to considering information handling and privacy compliance requirements; and
- the obligation to implement policies and practices to enable compliance with the Privacy Principles is to be qualified by a 'reasonable steps' test in recognition that 'the appropriate steps to take will depend upon the circumstances of each agency or organisation' thus adopting a 'risk-based approach'.

4.11 The Government response concluded:

> This additional supporting obligation to the 'openness' principle would expressly recognise what is only implicit in the existing Privacy Principles: that agencies and organisations need to take positive steps to ensure they comply with the Privacy Principles. However, it reflects what many agencies and organisations currently do in practice to ensure they meet their

9 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. 48.

> obligations under the Privacy Act. It is therefore not intended to impose any unreasonable additional burden on agencies and organisations.[10]

Issues

4.12 The ALRC, OPC, Privacy NSW and the Australian Institute of Credit Management welcomed the positioning of the openness and transparency principle as the first APP. Professor Rosalind Croucher, President, ALRC, commented further:

> It brings it up to the front as the first principle and provides, as I described it in the submission, a conceptual mirror to the idea of openness that is captured in the freedom of information legislation. That is a good initiative and we commend the introduction of the principles in that fashion.[11]

4.13 Support was expressed for the Government's aim of encouraging entities to manage personal information openly and transparently, as well as the aim of ensuring that entities take reasonable steps to comply with the Privacy Act and to handle complaints. The Government's intention to ensure that entities undertake appropriate planning prior to the point of dealing with personal information, and when planning new information systems, was also welcomed.[12] However, in order to ensure that this was stated more clearly, the NSW Department of Justice and Attorney General suggested that APP 1(2) be re-titled 'Planning for compliance with the Australian Privacy Principles'.[13]

4.14 The committee also received submissions that did not support the notion that the privacy obligations could, or should, be considered when entities design information systems, that is, the 'privacy by design approach'. Microsoft commented that 'it could be hard to read privacy by design elements into the principle as currently worded'. Microsoft went on to state that it would be wary about trying to load this concept into the principle as it is difficult to see how it would be defined or enforced. In addition, it would raise 'real possibilities of inappropriate government interventions into what should properly be business decisions'. Microsoft also pointed to comments by European Union Data Protection Supervisor, Mr Peter Hustinx, who saw privacy by design not as a matter of law, but something that would be achieved through the practices of organisations. Microsoft supported this view and concluded that legislating for privacy by design would be 'onerous, impractical and would have real potential to stifle innovation'.[14]

---

10 Australian Government, *Enhancing National Privacy Protection*, pp 48–50.

11 Professor Rosalind Croucher, President, Australian Law Reform Commission, *Committee Hansard*, 25 November 2010, p. 1.

12 Office of the Privacy Commissioner, *Submission 39*, p. 23; Privacy NSW, *Submission 29*, p. 3; Australian Institute of Credit Management, *Submission 8*, p. 2.

13 NSW Department of Justice and Attorney General, *Submission 42*, p. 2.

14 Microsoft, *Submission 14*, p. 9.

4.15 The Office of the Information Commissioner Queensland (OIC) drew attention to the inclusion of a 'reasonable in the circumstances' test in APP 1 and commented that it did not consider that the obligation to comply with the privacy principles should be subject to such a test. The OIC argued that state and territory jurisdictions, which have enacted information privacy laws, impose a mandatory requirement to comply with the relevant privacy principles. In addition, the OIC commented that the adaptable and flexible nature of the APPs provides sufficient scope for entities to implement them in ways which are reasonable, based on the circumstances and context of the entity's personal information handling. As such the OIC recommended that the committee consider APP 1 in terms of whether or not it would be more appropriately stated as a mandatory obligation.[15]

Conclusion

4.16 The committee considers that by placing the 'openness' principle as the first APP, attention is drawn to the need to manage personal information in an open and transparent way. The Government has included in APP 1 an obligation to develop and implement internal policies and practices that enable compliance with the privacy principles. This will strengthen the 'openness' principle and encourage a proactive approach to privacy compliance. The committee believes that by requiring the planning of data systems to take account of privacy requirements, the handling of personal information will be improved and individuals will be confident that entities have taken all necessary steps to provide adequate systems to protect their personal information. Further, the committee does not agree that the 'privacy by design' approach will stifle innovation. Rather, as technology is advancing so rapidly, what is regarded as 'innovation' may in fact pose significant risks to privacy, and thus privacy obligations should be a fundamental consideration in planning information systems.

4.17 The committee also considers that the inclusion of a test of reasonableness ensures that entities have flexibility in the way in which they address the obligations under this principle and, as stated in the Government response, recognises that the appropriate steps to take will depend upon the circumstances of each agency or organisation. In addition, the committee notes that the Government commented in its response to the ALRC's recommendations that:

> In this way, the additional requirement adopts a risk-based approach, whereby an agency or organisation would consider what internal practices and policies to implement with regard to such matters as the volume of personal information it handles, the sensitivity of that information and the purpose for which the information is collected, used and disclosed.
>
> In addition to considering the level of risk in their information handling needs and practices, agencies and organisations would also consider what is reasonable for them to do with regard to their size and available resources,

15 Office of the Information Commissioner Queensland, *Submission 18*, p. 2.

> the type of functions or activities they undertake, and the extent to which they have already established internal policies and practices.[16]

4.18 The committee concurs with this approach.

Structure and terminology

4.19 Submitters commented on the structure of, and the terminology used in, APP 1. The Law Institute of Victoria (LIV) suggested that, to ensure consistency with APP 1(3) which requires an entity to have 'up-to-date policy' on the management of personal information, APP 1(2) should be amended to read 'implement and review practices'.[17]

4.20 The Law Council of Australia (LCA) commented on the terms used in APP 1(2)(a). First, the LCA was concerned about the strength and the mandatory nature of the language used. Secondly, the LCA noted that APP 1(2)(a) requires an entity to take 'such steps as are reasonable in the circumstances to implement practices, procedures and systems that will ensure that the entity complies with the Australian Privacy Principles'. The LCA suggested that it is not possible for 'practices, procedures and systems' to ensure compliance with the APPs. In order to address this matter, the LCA suggested replacing the word 'will ensure' with words such as 'have the primary purpose of promoting compliance'.[18]

4.21 The department responded to the LCA's comments and stated that, by including the 'will ensure' formula, the Government has gone further than the ALRC recommendation 'in requiring agencies and organisations not only to create and maintain a privacy policy but to also demonstrate that they have taken reasonable steps to comply with both the privacy principles and their own privacy policy'.

4.22 The department went on to state that the term the 'primary purpose of promoting' provides for a different requirement than the term 'will ensure'. The department argued that the terms of APP 1(2)(a) provide a clear requirement for entities to have practices, procedures and systems that will ensure compliance with the APPs. The term suggested by the LCA was seen as a lesser obligation and 'is not consistent with the Government's approach of promoting high standards of compliance that will require entities to consider how the principles apply to their own circumstances and what steps it should take to implement appropriate policies and practices'. The department concluded that:

> It was the Government's intention for the compliance standards on agencies and organisations to be sufficiently high to enhance privacy protections.

16 Australian Government, *Enhancing National Privacy Protection*, p. 50.

17 Law Institute of Victoria, *Submission 36*, p. 4.

18 Law Council of Australia, *Submission 31*, p. 4.

> The 'will ensure' obligation was included so that privacy protections are built into the design of an entity's system and not 'bolted on' afterwards.[19]

4.23 Microsoft put the view that APP 1(2) is redundant. Microsoft noted that section 16A of the *Privacy Act 1988* provides that 'an organisation must not do an act, or engage in a practice, that breaches a National Privacy Principle'. If, it was argued, a modified version of section 16A is to be enacted to prohibit breaches of the APPs, regulated entities will be required to take steps to comply with the APPs and thus APP 1(2) is redundant. Microsoft concluded:

> If APP [1(2)] was enacted as proposed, it would be possible for an entity to be liable for breaching APP [1(2)] simply because it had not prepared a document that described the procedures it would take with the objective of ensuring compliance with the remainder of the APPs. This would be so even if there had been no breach by the entity of any of the substantive APPs…
>
> We just do not believe that APP [1(2)] will assist individuals whose privacy is at risk of being interfered with - they will have remedies if and when a breach of the substantive principles occurs. In a case involving serious and systematic breaches of the APPs, a court has power under section 98 of the Privacy Act to require an entity to take positive steps to prevent future breaches. This power would likely extend to introducing a compliance program - similar orders are commonly made at the request of the ACCC in cases involving contraventions of the Trade Practices Act.[20]

4.24 The OPC also commented on the complexity of the term 'steps as are reasonable in the circumstance' used in APP 1 and other APPs.[21] The committee has addressed these comments in its discussion on the complexity of the APPs in chapter 3.

Privacy policy requirements

4.25 APP 1 also sets out the requirements for an entity's privacy policy: first, that it must be clearly expressed and up-to-date (APP 1(3)); and secondly, that it must contain certain information (APP 1(4)). These provisions were supported by the Health Services Commissioner, Victoria, who noted that the provisions of APP 1 go further than the existing provisions in the Privacy Act and the equivalent provisions in the Victorian Health Records Act.[22] Similarly, the Office of the Victorian Privacy Commission supported the more prescriptive nature of APP 1 as 'it will better allow individuals to identify precisely how entities intend to handle personal information'.[23]

---

19 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 6.

20 Microsoft, *Submission 14*, p. 9.

21 Office of the Privacy Commissioner, *Submission 39*, p. 23.

22 Health Services Commissioner, Victoria, *Submission 26*, p. 2.

23 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 3

4.26 The committee received comments suggesting improvements to the privacy policy provisions. Professor Graham Greenleaf and Mr Nigel Waters, in their joint submission, commented on the need to make the list of matters to be included in an entity's privacy policy more consistent with the list of matters to be notified when collecting personal information under APP 5. For example, APP 1(4) requires information about how an individual may access information (d) and complain (e), but not 'identity and contact details' (APP 5(2)(a)).[24]

4.27 The NSW Department of Justice and Attorney General suggested that privacy policies should also provide some description of the individuals or entities who are likely to receive personal information and commented that 'this is crucial in terms of giving members of the public a real picture of how personal information is handled and to answer the question: "who are they giving it to?".' It was argued that such a requirement would complement the obligations under the disclosure principle (APP 5(f)).[25]

4.28 Other submitters, however, raised a range of concerns about the prescriptive nature of the information to be included in an entity's privacy policy. For example, the LCA suggested that the privacy policy should only be required to contain 'reasonable information' or 'general information' about the various matters listed.[26]

4.29 The Australian Finance Conference (AFC) also commented that the prescriptive approach was at odds with the objective of providing high level principles and recommended that APP 1(4) be omitted entirely. Both the Australian Association of National Advertisers (AANA) and AFC recommended that the guidance on content of privacy policies be left to the Australian Information Commissioner.[27] Similarly, the AANA submitted that the provisions in relation to privacy policies be limited to core information requirements and that guidance, as is currently the case, be developed to assist entities in meeting their obligations.[28]

4.30 Microsoft's comments concerning APP 1(4) were based on 'evidence that individuals can be overwhelmed but not enlightened by long privacy policies or disclosure statements, even where intended to allow informed consent'. Microsoft submitted that layered privacy notices were one way of improving understanding of privacy policies by providing clear and concise summaries with links to the full privacy statement for those interested in more detailed information. Microsoft suggested APP 1(3)–1(6) (and APP 5) be streamlined by focusing on identifying transparency objectives. Organisations could then choose how best to communicate with individuals to meet these objectives in an effective and cost efficient way.

---

24 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 5.

25 NSW Department of Justice and Attorney General, *Submission 42*, p. 2.

26 Law Council of Australia, *Submission 33*, p. 4.

27 Australian Finance Conference, *Submission 12*, p. 3.

28 Australian Association of National Advertisers, *Submission 21*, p. 6.

Microsoft concluded that 'this would help reduce the compliance burden on organisations and reduce the load on individuals'.[29]

4.31 A range of comments were received in relation to APP 1(4)(g) which requires that if an entity is likely to disclose personal information to overseas recipients, the entity's privacy policy must, if it is practicable to do so, contain the countries in which such recipients are likely to be located. The inclusion of this requirement was supported by Privacy NSW.[30] In addition, Professor Greenleaf and Mr Waters argued that the inclusion of the term 'if it is practicable to specify those countries' provided a far too subjective qualification, and 'is likely to lead to many entities not including this important information'. It was suggested that entities, which do not include this information, be required to give an explanation as to why countries were not specified in the privacy policy.[31]

4.32 Other submitters did not support the inclusion of the obligation under APP 1(4)(g). It was argued that to comply with the obligation was impractical, onerous and costly.[32] Submitters, for example, Yahoo!7 and the Australian Bankers' Association (ABA), commented on the obligations imposed by APP 1(4)(g) for those entities which use overseas servers and cloud computing. It was argued that it was impractical to list all countries, with the ABA noting that banks do not control the location of an overseas server and the server's location may change without the bank's knowledge. The ABA argued that to keep track of these changes, and to continuously update privacy policies, would be onerous and costly.[33]

4.33 The ABA also suggested that APP 1(4)(g) may lead to an individual drawing an incorrect inference that a country named as the location of the intended overseas recipient is not to be trusted with the personal information and 'this would be an unfortunate signal for Australia's law to send internationally'.[34]

4.34 A number of suggestions to address concerns with APP 1(4)(g) were put to the committee. Yahoo!7 favoured a simple disclosure obligation which referred to international data transfer and backup more generally.[35] However, Telstra suggested that the use of very broad references and catch-alls in a privacy notice would diminish

29 Microsoft, *Submission 14*, pp 9–11.

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

31 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 5; Attachment 1, p. 4.

32 See for example, Australian Bankers' Association, *Submission 15*, p. 3.

33 Australian Bankers' Association, *Submission 15*, p. 3; see also Telstra Corporation Ltd, *Submission 19*, p.1.

34 Australian Bankers' Association, *Submission 15*, p. 3.

35 Yahoo!7, *Submission 20*, p. 1.

the value of providing the information and may lead to confusion. Thus, Telstra argued that APP 1(4)(g) should be omitted.[36]

4.35 The ABA suggested the addition of the words 'reasonable and' before the word 'practicable' to take into account potential volatility in the location of servers in other countries.[37] A number of submitters suggested that as APP 8 deals specifically with cross-border disclosure of personal information APP 1(4)(g) is irrelevant.[38]

4.36 Again, concerns were raised that consumers would not be assisted by long and complex information, specifically in relation to APP 1(4)(f) and (g). Privacy Law Consulting was also of the view that there may be limited benefit to consumers of the provisions as 'they do not result in consumers being provided with a level of information that will enable them to properly consider privacy issues associated with the overseas disclosure'.[39] The AANA also commented that APP 1(4)(f) and (g) 'are unnecessary and not useful information to an individual'. Rather, the AANA submitted that 'the intent of these provisions is to alert individuals that an overseas recipient may not be subject to privacy legislation similar to that of Australia'.[40]

4.37 Privacy Law Consulting voiced concern with the requirement of APP (4)(f) and (g) in relation to the disclosure of commercially confidential information and stated that these obligations may result in the disclosure of details about an organisation's operational arrangements and 'inner-workings'. Privacy Law Consulting gave the example of the outsourcing of back-office functions such as accounts or dictation transcription and noted that such information is not normally made public.[41]

Conclusion

4.38 The committee considers that there are benefits in including in the APPs a list of requirements for privacy policies: it helps to promote transparency; provides consumers with a clear indication of what must be included in a privacy policy; and by having to provide clear privacy policies, entities will be required to examine how they handle personal information at each stage of the information cycle.

4.39 While the committee acknowledges concerns that such an approach may compromise the aim of high-level principles in the Privacy Act and that consumers do not always comprehend overly long privacy policies, the committee considers that the benefits to transparency and overall compliance with the privacy principles outweigh

---

36 Telstra Corporation Ltd, *Submission 19*, p.1.

37 Australian Bankers' Association, *Submission 15*, p. 3.

38 National Australia Bank, *Submission 2*, p. 2; Australian Bankers' Association, *Submission 15*, p. 3.

39 Privacy Law Consulting, *Submission 24*, p. 1.

40 Australian Association of National Advertisers, *Submission 21*, p. 6.

41 Privacy Law Consulting, *Submission 24*, p. 1.

these concerns. The committee considers it is important that the principle provides for the minimum amount of information that is required in a privacy policy and makes it clear that it is not exhaustive and that further information must be included as the particular circumstances of the entity require. On balance, the committee therefore supports the inclusion of the matters to be addressed by a privacy policy within the body of the principle. The committee also notes that the Government encourages the Office of the Australian Information Commissioner to provide guidance in this matter.

4.40 In relation to APP 1(4)(g), the committee considers that many consumers have concerns about the transfer of personal information overseas and that this practice is increasing as technology changes and global markets expand. The committee therefore believes that privacy policies should include information if an entity is likely to disclose personal information to an overseas entity and the countries in which such recipients are likely to be located. The committee notes that APP 1(4)(g) contains the proviso that 'if it is practicable to specify those countries in the privacy policy'. The committee considers that this provides sufficient flexibility to address concerns raised by Yahoo!7 and the Australian Bankers Association.

Availability of privacy policy

4.41 Both the NSW Department of Justice and Attorney General and Professor Greenleaf and Mr Waters commented that the proposal that an entity's privacy policy need only be made available 'in such form as is appropriate' (APP 1(5)(b)) was different to the ALRC's recommendation that access must be provided 'electronically'. Professor Greenleaf and Mr Waters argued that the proposed provision was both weaker and inferior and went on to argue that the requirement in APP 1(6) for entities to respond to an individual's request for the policy in 'a particular form' is only a partial and relatively weak substitute.[42] The NSW Department of Justice and Attorney General commented that:

> In the interests of transparency and accountability, APP1 could explicitly state that entities should take reasonable steps to make the policy available electronically. In practice, this will most likely result in policies being posted on the websites of entities that have them. This is likely to be the first place members of the public will look for privacy policies and it may be appropriate to make explicit the requirement to make them available in this manner.[43]

4.42 The department responded to concerns about APP 1(5) and stated that it believed that an absolute requirement to provide the privacy policy electronically would be a significant burden on organisations without a website or means to otherwise produce an electronic copy. The department went on to state that APP 1(5)(b) puts agencies and organisations under an obligation to provide an appropriate copy of their privacy policy in a way which is reasonable in all the

42 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 6.

43 NSW Department of Justice and Attorney General, *Submission 42*, p. 2.

circumstances, having regard to the agencies' or organisations' functions, types of business and restrictions. It also addresses issues around accessibility; for example, clients of some entities may not have computers and therefore are unable to electronically access privacy policies. The department concluded that, as a consequence, there should be the option available of providing the policy in any other appropriate format.[44]

4.43 Professor Greenleaf and Mr Waters also suggested that it was undesirable for APP 1(6) to apply only to requests from individuals as often organisations such as NGOs and the media may seek access to privacy policies, and this should be expressly accommodated.[45] In response to this suggestion, the department stated the provision is based on ALRC recommendation 24-2, which also uses the terminology 'individual'. While there is no definition for 'individual' in either the APPs or the ALRC Report, paragraph 22(1)(aa) of the Acts Interpretations Act defines an 'individual' as a 'natural person'. The department went on to state that there is nothing preventing an individual within an organisation, or the media, from making the request and concluded:

> Therefore, in practice, there should be no foreseeable problem in media or organisations gaining access to relevant documents containing the Privacy Policies of an agency or organisation.
>
> It is not the Government's intention to prevent organisations from making requests for an entity's privacy policy. Therefore, the Department will consider the Senate Committee's recommendations on this issue, including suggestions for improving clarity on this issue.[46]

Conclusion

4.44 The committee considers the requirement for an entity to make its privacy policy available 'in such form as appropriate' should be further clarified by the inclusion of a note at the end of APP 5 indicating that the form as is appropriate will usually be an online privacy policy. In relation to concerns about access to privacy policies by organisations including the media, the committee does not believe that an entity would deny access through a narrow reading of the provisions of APP 1(6). However, to ensure that the intent of the provision is clear, the committee considers that the provision be re-drafted to clarify that privacy policies must be available to both individuals and entities.

Recommendation 6

4.45 The committee recommends that a note be added at the end of APP 1(5) which indicates that the form of an entity's privacy policy 'as is appropriate' will usually be an online privacy policy.

---

44 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 6.

45 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 6.

46 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 7.