Chapter 14

Australian Privacy Principle 11–security of personal information

Introduction

14.1 Australian Privacy Principle 11 (APP 11) protects personal information by imposing specific obligations on both agencies and organisations which hold that information. The principle also provides that entities take reasonable steps to destroy or de-identify the personal information once it is no longer needed. The Companion Guide noted that keeping personal information for only as long as 'reasonably necessary is an effective way of reducing the risk that it may be mishandled'. In addition, these obligations are in line with international best practice on privacy protection.[1]

Background

14.2 There are currently requirements within the National Privacy Principles (NPPs) and Information Privacy Principles (IPPs) which ensure agencies and organisations protect the personal information in their possession. NPP 4 requires organisations to take reasonable steps to protect personal information from misuse and loss and from unauthorised access, modification or disclosure as well as taking reasonable steps to destroy or de-identify information no longer needed.

14.3 IPP 4 requires that personal information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse. If the personal information is provided to a service provider, everything reasonably within the power of the agency is to be done to prevent unauthorised use or disclosure of information contained in the record.

14.4 The Australian Law Reform Commission (ALRC) noted the importance of a data security principle in privacy legislation, which is reflected by the provisions set out for both agencies and organisations to 'take reasonable steps to maintain the security of the personal information that they hold'. In addition, there are a number of international instruments relating to privacy which ensure the security of personal information.[2]

14.5 The ALRC review focussed on:

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, p. 14.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 941–942.

- how agencies and organisations should fulfil their data security obligations during the active life of records that contain personal information;
- disclosure of personal information to third parties; and
- the obligations of agencies and organisations to destroy or render non-identifiable personal information when it is no longer needed.

14.6 The ALRC recommended the data security principles be consolidated and simplified into a single principle. However, the ALRC commented that a consolidated principle would 'need to be sufficiently flexible to accommodate the differences' between the functions of the private sector and the public sector.[3]

14.7 The ALRC went on to comment that the criteria in the principle should ensure that personal information is 'protected from misuse and loss and from unauthorised access, modification or disclosure'. The ALRC explained that 'these criteria balance the role of the "Data Security" principle and those acts and practices that can be regulated more appropriately through other privacy principles'. Furthermore, the ALRC noted that some authorised access, use and disclosure can be improper and would not be regulated by the criteria above and are regulated elsewhere in the privacy principles by the data quality and use and disclosure principles.[4]

14.8 The ALRC also commented on the issue of personal information exchanged over the internet and whether it should be regulated by provisions in this principle. However, in keeping with the recommendation to keep the privacy principles technologically neutral, the ALRC considered that this step would not be necessary.[5]

14.9 In relation to the requirement on entities to take 'reasonable steps' to prevent the loss and misuse of personal information, the ALRC commented that 'implementing privacy-enhancing technologies will be one of the main ways through which agencies and organisations will comply with the requirement'. The ALRC acknowledged concerns by the Office of the Privacy Commissioner (OPC) on providing appropriate guidance on technological developments and recommended 'that the *Privacy Act* be amended to empower the Privacy Commissioner to establish expert panels at his or her discretion' to provide guidance on privacy-enhancing technologies.[6]

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 944.

4 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 949.

5 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 949.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 950.

14.10 The ALRC considered the requirement of IPP 4 that provides that if an agency discloses personal information to a third party to carry out a service, the agency is required to take steps to prevent the unauthorised use and disclosure of this personal information by the third party involved. The ALRC did not recommend that such a requirement be included in the 'Data Security' principle. It noted that agencies remain regulated by section 95B of the Privacy Act[7] which provides that an 'agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles'. However, the ALRC commented that its position assumed implementation of a number of other recommendations including removal of the small business exemption from the Privacy Act and changes to the cross-border flow of data provisions. If these recommendations are implemented, the ALRC concluded that 'there will be few, if any, situations where a contracted party will not be under an obligation to comply with the Privacy Act.[8]

14.11 However, the ALRC remarked that if the above recommendations are not implemented 'then a requirement for organisations to take steps to protect information disclosed to a third party...will be an integral component of the *Privacy Act*'.[9]

14.12 In relation to the provision to de-identify personal information that is no longer needed, the ALRC recommended the phrase 'render de-identifiable' be used instead the NPP 4 wording of 'permanently de-identify'. The ALRC noted that this rephrasing would make it clearer that data destruction should include the prevention of re-identification of data in the future.[10]

14.13 Another concern raised during the ALRC review was the possible conflicts between the requirement to destroy data and the requirements of agencies to retain information. According to the ALRC, '[t]he data destruction requirement included in the "Data Security" principle must be worded so as to accommodate the various reasons why agencies and organisations may need to retain personal information'.[11] The ALRC noted that agencies are prohibited by the *Archives Act 1983* to destroy Commonwealth records without the permission of the National Archives, subject to certain exceptions. The ALRC noted however that the interaction between subsection 24(2) of the Archives Act and the destruction requirements of the Privacy Act were

---

7 'This section requires an agency entering into a Commonwealth contract to take contractual measures to ensure that a contracted service provider for the contract does not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency', *Privacy Act 1988*, p. 187.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 954–55.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 955.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 958.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 963–965.

not clear. The ALRC recommended that 'agencies responsibilities under the *Archives Act* should take precedence over the data destruction requirement in the data security principle'.[12]

14.14 Another issue raised in the ALRC review was the concept of giving an individual the right to request an agency or organisation to destroy personal information that relates to that individual. The ALRC did not support this approach to data destruction, noting that it would be too rigid and would encourage destruction even when another method of dealing with the information may be more appropriate for example, rendering the information non-identifiable. The ALRC noted that rendering information non-identifiable still allows entities to evaluate the effectiveness of their projects, while not conflicting with the archives legislation obligations and ensuring that personal information is secure.[13]

14.15 In relation to guidance, the ALRC recommended that the OPC develop and publish guidance on matters including what constitutes 'reasonable steps' to prevent the misuse and loss of personal information by organisations and agencies; when it is appropriate to destroy or render non-identifiable personal information; the interaction between the data destruction requirements and legislative records retention requirements; and the manner in which personal information should be destroyed or rendered non-identifiable.[14]

Government Response

14.16 The Government responded positively to all the recommendations made by the ALRC in regards to the data security principle. The Government accepted that a data security principle should ensure the protection of personal information from loss and misuse, as well as the requirement to destroy and render non-identifiable information that is no longer needed. The Government noted that in relation to data destruction, the requirements on agencies to destroy or retain information as set out by the *Archives Act 1983* would not be affected.

14.17 The response supported the ALRC recommendations to have the OPC develop and publish guidelines on what constitutes 'reasonable steps' and the expected requirements on entities to destroy or render personal information non-identifiable.[15]

---

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 965.

13 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 967.

14 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 951; p. 970.

15 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, pp 62–63.

Issues

14.18 The issue of security of personal information was important to many of the submitters to this inquiry. Microsoft commented that 'security as an absolutely critical element of a privacy framework. Poor security makes privacy impossible.'[16] The Office of the Victorian Privacy Commission welcomed APP 11, remarking that it largely mirrors NPP 4 and Victorian IPP 4.[17] Similarly, the Australian Institute of Credit Management supported this principle and Yahoo!7 broadly agreed with its flexible approach.[18]

Structure

14.19 As discussed in the previous chapter, Privacy NSW suggested that APP 10 and APP 11 should be relocated within the legislation to better reflect the information cycle, that is, the quality principle and the security principle should be placed after the notification principle and before the use and disclosure principle.[19]

Protecting personal information

14.20 APP 11(1) provides that an entity must take such steps as are reasonable in the circumstance to protect information from misuse, interference and loss and from unauthorised access, modification or disclosure. The Office of the Health Services Commissioner Victoria indicated support for APP 11(1) as did the Australian Bankers' Association (ABA) which welcomed the stronger emphasis on 'organisations to take all reasonable steps to ensure their systems and processes are secure'.[20] Other submitters commented on the 'reasonable steps' requirement, the protection of information accessed by contractors to agencies, and the inclusion of the term 'interference'.[21]

14.21 Microsoft submitted that 'getting security right is a bit more objective than some other aspects of privacy' and that the APPs could 'accommodate some more specific tests provided these did not affect cost effectiveness and were conducive to innovation'. In support of this view, Microsoft suggested 'a specified list of factors in the data security principle to help guide any determinations as to whether an organisation has taken "reasonable steps" to secure personal information it holds'.

---

16 Microsoft Australia, *Submission 14*, p. 12.

17 Office of the Victorian Privacy Commissioner, *Submission 5*, p. 9.

18 Australian Institute of Credit Management, *Submission 8*, p. 4; Yahoo!7, *Submission 20*, p. 3.

19 Privacy NSW, *Submission 29*, p. 8.

20 Office of the Health Services Commissioner Victoria, *Submission 26*, p. 4; Australian Bankers' Association, *Submission 15*, p. 14.

21 Australian Bankers' Association, *Submission 15*, p. 14; Telstra Corporation Ltd, *Submission 19*, p. 4; Australian Direct Marketing Association, *Submission 27*, p. 10; Privacy Law Consulting, *Submission 24*, p. 3 & p. 9; Office of the Health Services Commissioner Victoria, *Submission 26*, pp 4–5; Financial Services Council, *Submission 34*, pp. 3–4.

Microsoft has suggested this list be included in the legislation, or at least included with guidance issued by the Office of the Australian Information Commissioner once the legislation is in place.[22]

14.22 The NSW Department of Justice and Attorney General commented on the security requirements for information held by agencies which may be accessed by a contractor. It noted that, under section 95B of the Privacy Act, an agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles. However, APP 11 imposes no such requirement. While many organisations will be subject to APP 11, the small business exemption means that some organisations which may handle very sensitive personal information will not fall within the ambit of APP 11. The NSW Department of Justice and Attorney General recommended that consideration be given to replicating the requirement imposed on agencies by section 95B (and NSW legislation) 'in any model privacy laws if it is not to be provided for in the APPs'.[23]

14.23 The security of information in the hands of a contractor was also raised by the Privacy Interest Advocacy Centre (PIAC) in its submission to the ALRC review. PIAC stated that it was important to 'ensure that the data disclosed to third parties under contractual arrangements is maintained'.[24]

14.24 The National Association of Information Destruction (NAID-Australasia) suggested that APP 11 include a direction to entities that data protection policies and procedures be documented in writing. NAID-Australasia suggested that benefits would arise from such a requirement: having written policies and procedures is the only way to ensure that employees and vendors are given proper direction; and written policies and procedures is the only way an entity can demonstrate that it comprehends and takes its responsibilities to protect personal information seriously.[25]

Use of the term 'interference'

14.25 The ABA commented on the inclusion of the term 'interference' in APP 11(1)(a), and noted it is not present in the corresponding NPP. The ABA stated that it is not clear what the term intends to address, and sought specific guidance, with examples, on how it may occur and how 'interference' differs from the other listed factors of 'misuse', 'unauthorised access' and 'modification'.[26] The Australian Direct Marketing Association (ADMA) also noted the inclusion of the new term 'interference' in APP 11 and commented that the term is used broadly and without

22 Microsoft Australia, *Submission 14*, p. 12.

23 NSW Department of Justice and Attorney General, *Submission 42*, p. 10.

24 Privacy Interest Advocacy Centre, *Submission 32*, Attachment, p. 11.

25 National Association for Information Destruction, *Submission 6*, p. 3.

26 Australian Bankers' Association, *Submission 15*, p. 14.

proper definition. ADMA sought further clarification on 'how broadly the obligations that stem from this inclusion would be expected to apply'.[27]

14.26 Telstra expressed a similar view and went on to state that 'interference' could be viewed as 'unlawful interception' which requires further technological protections and 'degrees of encryption'. Telstra commented this could 'unfairly impose responsibility for external events or attacks' on organisations and lose the technologically neutral objective of the legislation. Telstra suggested the removal of the term 'interference'.[28]

14.27 The Department of the Prime Minister and Cabinet responded to these concerns and stated:

> The inclusion of 'interference' in APP 11 is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information (such as attacks on computer systems). It is correct that this element may require additional measures to be taken to protect against computer attacks etc, but the requirement is conditional on steps being 'reasonable in the circumstances'. Practical measures by entities to protect against interference of this nature are becoming more commonplace.
>
> The use of the term 'interference', which focuses on the activity rather than the means of the activity, ensures that the technologically neutral approach to the APPs is retained.[29]

Destruction of personal information

14.28 APP 11(2) provides for the destruction of records no longer required. NAID-Australasia supported information destruction as being a reasonable precaution for the security of personal information. However, it noted that the concept of destruction is often misunderstood, and gave the example of organisations relying on 'casual disposal or simple recycling as methods of destruction'. In order to clarify the meaning of destruction, NAID-Australasia recommended a definition of destruction within the definition section of the legislation. NAID-Australasia believed 'it is possible to define "destruction" while remaining technologically neutral, reasonable and non-descriptive'.[30]

14.29 The Office of the Health Services Commissioner Victoria commented that the provisions of APP 11(2) are not appropriate for the health industry as 'there may be a lapse of time in people re-presenting for treatment, or there may be medical conditions that are slow to progress'. The Commission recommended that a minimum retention

---

27 Australian Direct Marketing Association, *Submission 27*, p. 10.

28 Telstra Corporations Ltd, *Submission 19*, p. 4.

29 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 28.

30 National Association for Information Destruction, *Submission 6*, pp 3–4.

period for records be included in this principle, as is the case in Victoria, where the *Health Records Act* provides for a minimum retention period of seven years for health records. The Commission recommended that state and federal laws should continue to operate side by side, to ensure the seven year retention period is maintained.[31]

14.30 The Financial Services Council (FSC) requested further guidance on when it is appropriate to destroy or de-identify personal information, and the 'interaction between data destruction requirements and legislative record retention requirements'. The Council stated that retaining records for seven to ten years from the last date of interaction with the client is standard practice in the financial services industry and recommended that the requirement to destroy or de-identify personal information 'commence after other legal requirements for record retention timeframes have been met'.[32]

14.31 Yahoo!7 suggested that the provisions for the retention of personal information rely on 'legitimate business purposes' rather than the purposes of APP 10 and APP 11.[33]

14.32 Google Australia stated that subsection APP (2)(c) should be amended to allow for compliance with foreign laws. Google noted that they conduct business worldwide and are required to comply with both Australian Privacy Laws and Foreign Privacy Laws.[34] (The committee has commented on this matter in chapter 3, see paragraphs 3.77–78.)

14.33 Privacy Law Consulting Australia raised concerns about this privacy principle conflicting with section 24 of the Archives Act and creating a circular process of interaction between the provisions of the two Acts. The Consultancy suggested including information within APP 11 to explain its interaction with section 24 of the Archives Act.[35] Similar points were raised by the ALRC (see para 14.18). The Government response stated that the ALRC's recommendation in relation to destruction or de-identifying information 'does not affect the operation of the *Archives Act 1983* on how agencies retain personal information'.[36]

Conclusions

14.34 The issue raised by the NSW Department of Justice and Attorney General and the Privacy Interest Advocacy Centre concerned the protection of information held by agencies which may be accessed by third parties, for example, contractors. The

---

31 Office of the Health Services Commissioner Victoria, *Submission 26*, pp 4–5.

32 Financial Services Council, *Submission 34*, pp 3–4.

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

34 Google Australia, *Submission 16*, pp 6–7.

35 Privacy Law Consulting, *Submission 24*, pp 3, 9.

36 Australian Government, *Enhancing National Privacy Protection*, p. 63.

committee notes that the ALRC did not recommend such a requirement. Further, the ALRC commented that agencies remain subject to section 95B of the Privacy Act which provides that an agency must take contractual measures to ensure that contracted service providers do not breach the privacy principles. The Government has not indicated that a provision similar to section 95B will not be retained in the new Act. However, the committee will consider this matter further when the relevant exposure draft is provided.

14.35 In relation to comments concerning the inclusion of the term 'interference' in APP 11(1)(a), in particular that its meaning is unclear, the committee notes that the department has indicated that 'interference' is intended to recognise that attacks on personal information may not be limited to misuse or loss, but may also interfere with the information in a way that does not amount to a modification of the content of the information. The department provided the example of 'interference' through an attack on a computer system. The committee considers that this is an essential protection for personal information and supports the inclusion of the term 'interference'. However, the committee believes compliance with this principle would be improved if the term 'interference' was defined or a note was included to explain its meaning.

Recommendation 24

14.36 The committee recommends that a definition of the term 'interference' used in proposed APP 11(1)(a), pertaining the security of personal information, be provided or a note included in the legislation to explain its meaning in this context.

14.37 The committee considers that the destruction of personal information no longer required is an important matter. The committee notes the concerns raised by NAID-Australasia that destruction of information is often misunderstood and approached in a less than appropriate manner. The committee considers that it will be important that guidance is provided in relation to what constitutes 'destruction' in relation to personal information. The committee also notes that submitters called for guidance on range of other matters and that the need for guidance from the Office of the Australian Information Commission was recommended by the ALRC and accepted by the Government.

Recommendation 25

14.38 The committee recommends that the Australian Information Commissioner provide guidance on the meaning of 'destruction' in relation to personal information no longer required and the appropriate methods of destruction of that information.

14.39 Submitters did not comment on the use of the term 'to ensure that the information is no longer personal information' in relation to APP 11 however, comments were made in relation to APP 4, see chapter 7.