Chapter 5

Australian Privacy Principle 2–anonymity and pseudonymity

Introduction

5.1 Australian Privacy Principle 2 (APP 2) ensures that individuals are permitted to interact with entities while not identifying themselves, or by using a pseudonym. The Companion Guide states that APP 2 emphasises the importance of first considering whether it is necessary to collect personal information at all. By doing so, privacy protection to individuals is improved as it prevents an entity from collecting personal information if it is not needed by the entity. APP 2 recognises that there are some instances where the entity is not necessarily interested in the identity of the individual but rather that the credentials of the individual have been sufficiently established for the purpose of the transaction.

5.2 Entities will only be required to comply with APP 2 where it is lawful to do so. If a law requires the individual to identify him/herself to the entity, then it is not lawful and practicable for them to interact anonymously or pseudonymously.

5.3 The Companion Guide indicates that the Australian Information Commissioner will be 'encouraged to provide guidance on the principle, including on the types of circumstances in which it will not be lawful or practicable to provide this option'.[1]

Background

5.4 National Privacy Principle 8 (NPP 8) requires that private sector organisations provide an opportunity to individuals, where lawful and practicable, to interact on an anonymous basis when a transaction is taking place. The Australian Law Reform Commission (ALRC) stated that this right 'is designed to give individuals, where appropriate, greater control over how much personal information they wish to reveal to organisations with which they are dealing'. In addition, it allows an individual, where applicable, to provide highly personal or intimate information to an entity with a minimal risk to having their identity traced or revealed.[2]

5.5 There is no comparable anonymity principle in the Information Privacy Principles although the privacy legislation of some state jurisdictions (Victoria,

---

1 Australian Government, *Companion Guide, Australian Privacy Principles,* June 2010, pp 9–10.

2 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 689.

Tasmania and the Northern Territory) contain an anonymity principle that is applicable to public sector bodies.[3]

5.6 Both submitters to the Senate Legal and Constitutional Affairs References Committee 2005 inquiry into the *Privacy Act 1988* and the ALRC review called for the strengthening of the anonymity provisions in privacy legislation.[4]

5.7 In its submission to the Legal and Constitutional Affairs Committee, the Australian Privacy Foundation (APF) commented that the provision had failed to live up to its potential as a significant protection device, due partly to inadequate promotion and enforcement. It was noted that NPP 8 needed to be implemented at the design stage of initiatives so that claims of 'impracticability' could not be used for not offering an anonymous option. The APF also recommended a pseudonymous option as the next best practice where anonymity is either impracticable or unlawful.[5]

5.8 The ALCR review focussed on:

- whether the anonymity principle should be extended to public sector agencies;
- whether pseudonymity should be included in the principle; and
- what should be contained in the model Unified Privacy Principle (UPP).

5.9 The ALRC formed the view that the anonymity principle should be extended to public sector agencies. In coming to this view, the ALRC commented that an anonymity principle 'encourages agencies and organisations to consider the fundamental question of whether they need to collect personal information at all and to design their systems accordingly'. In addition, the ALRC argued that an option for dealing with agencies anonymously may potentially give rise to significant public policy benefits, for example, by encouraging individuals to seek medical or other assistance from agencies when they may not have been inclined to do so if they were required to identify themselves.[6]

5.10 The ALRC reported that during its review, the addition of a pseudonymity option was generally supported, particularly in the online environment. The ALRC therefore recommended that the anonymity principle should provide for pseudonymous transactions. The ALRC commented:

---

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 690.

4 Senate Legal and Constitutional Affairs References Committee, Inquiry into the *Privacy Act 1988,* Electronic Frontiers Australia, *Submission 17,* p. 44; Australian Privacy Foundation, *Submission 32,* p. 17.

5 Senate Legal and Constitutional Affairs References Committee, Inquiry into the *Privacy Act 1988,* Australian Privacy Foundation, *Submission 32,* p. 17.

6 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 693.

> This provides a more flexible application of the principle, by covering the situation where it would be impracticable or unlawful for an individual to transact anonymously but where these barriers would be overcome if the individual were to transact pseudonymously with an agency or organisation. An extension of the principle to encompass pseudonymous transactions will also encourage agencies and organisations to incorporate into their systems privacy-enhancing technologies that facilitate pseudonymous interactions in an online environment.[7]

5.11 The ALRC saw the anonymity option being available in instances where an entity did not need to contact the individual in the future. Where some form of identifier is required, but need not be personal information, pseudonymity is likely to be appropriate.

5.12 The ALRC noted that there was widespread concern about the practical application on the anonymity and pseudonymity principle which ranged from conflict with legislative requirements on an organisation to retain identifying information, to possible misuse of the 'practicable' element to avoid the principle completely.[8] The ALRC was of the view that the best way to address these concerns was to clarify the principle by using 'interacting' with an entity rather than 'transacting' as contained in NPP 8. The ALRC was also of the view that additional certainty was needed for the 'lawful and practicable' requirements.[9]

5.13 It was also the ALRC's view that agencies and organisations need to give a 'clear' option to interact anonymously or pseudonymously as this 'represents an appropriate balance between the interest in making individuals aware of their option to not identify themselves, or identify themselves pseudonymously, and the need to limit the cost of compliance for agencies and organisations'.[10] The ALRC also stated that the onus should be on agencies and organisation to give individuals options to interact anonymously and pseudonymously.[11]

5.14 In relation to guidance, the ALRC recommended that the Office of the Privacy Commissioner (OPC) should develop and publish guidance on:

---

7 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 696.

8 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 696–700.

9 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, pp 700–701.

10 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 705.

11 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 706.

(a) when it is and is not 'lawful and practicable' to give individuals the option to interact anonymously or pseudonymously with agencies or organisations;

(b) what is involved in providing a 'clear option' to interact anonymously or pseudonymously; and

(c) the difference between providing individuals with the option to interact anonymously and pseudonymously.[12]

Government response

5.15 The Government accepted both ALRC recommendations in relation to anonymity and pseudonymity. The Government response stated that anonymity and pseudonymity, limited to where lawful and practicable, are 'an effective way to protect individuals' privacy by ensuring that personal information is only collected where necessary'. In addition, the Government response stated that guidance on the issue will be very important in explaining that the right to interact anonymously or pseudonymously is limited to where it is lawful and practicable in the circumstances. The response also noted that it would be a decision for the Privacy Commissioner to provide guidance.[13]

Issues

5.16 This principle was generally welcomed by submitters.[14] The Office of the Victorian Privacy Commissioner noted the benefits of an individual having the option to interact anonymously or pseudonymously with an entity and stated:

> Where an organisation allows individuals to transact anonymously, the benefits are mutual. The individual transacts without giving up any control over his or her personal information. The entity will not incur any of the obligations that follow from collection of personal information under the other APPs…Providing an anonymity option is also consistent with the principle that an organisation or agency should not collect personal information unless this is necessary for one or more of its functions or activities.[15]

5.17 The Communications Council stated that APP 2 would significantly impact on the way in which entities interact with individuals, particularly in the online

12 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, ALRC 108, 2008, p. 708.

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. 39.

14 See for example, Health Services Commissioner, Victoria, *Submission 26*, p. 2; Privacy NSW, *Submission 29*, p. 3; Internet Society of Australia, *Submission 41*, p. 2.

15 Office of the Victorian Privacy Commissioner, *Submission 5*, pp 3–4.

environment. The Council noted that entities will need to first consider whether it is necessary to collect personal information and 'this is likely to call into review, and ultimately limit, the circumstances in which entities can request personal information from individuals'.[16]

5.18 Abacus Australian Mutuals and the Australian Bankers' Association also supported APP 2 as it was seen as providing greater clarity to financial institutions when they decline customers' requests to undertake transactions anonymously or pseudonymously because of obligations under anti-money laundering and counter terrorism laws.[17] The Internet Society of Australia (isoc-au) commented that increasingly, individuals must complete 'required information fields' on a website before they will be provided with information or before a transaction is finalised. A provision allowing for pseudonymity ensures that transactions can be completed without unnecessary personal information being provided.[18]

Structure and terminology

5.19 In relation to APP 2, Qantas commented that it replaced NPP 8 which, it contended, used much simpler language. Qantas concluded that it was difficult to see why it was necessary to replace NPP 8 when the meaning is unchanged.[19]

Provision of a 'clear option'

5.20 There was concern amongst some submitters that, contrary to the ALRC's recommendation and the Government response, APP 2 did not provide a 'clear option' for individuals to interact anonymously or pseudonymously where it is 'lawful and practicable in the circumstances'.[20] There were two matters raised: first, that APP 2 could be read as only requiring either the option of anonymity or pseudonymity, not both; and secondly, that the exceptions in APP 2(2) could be used to undermine the intent of the principle.

5.21 Submitters commented that APP 2 should be drafted to ensure that both options be available. The NSW Department of Justice and Attorney General stated that clarity could be gained by replacing the term 'or' with the term 'and'. However, it further commented that if one option is not practicable, there could be an exception from the requirements.[21]

---

16 The Communications Council, *Submission 23,* p. 9.

17 Abacus Australian Mutuals, *Submission 7,* p. 1; Australian Bankers' Association, *Submission 15,* p. 4.

18 Internet Society of Australia, *Submission 41,* p. 2.

19 Qantas, *Submission 38,* p. 3.

20 Office of the Privacy Commissioner, *Submission 39,* p. 24.

21 NSW Department of Justice and Attorney General, *Submission 42,* p. 3.

5.22 Professor Graham Greenleaf and Mr Nigel Waters also argued that the wording of APP 2 may allow entities to offer only pseudonymity rather than anonymity or pseudonymity. Professor Greenleaf and Mr Waters submitted an amendment to APP 2 which they considered would overcome these identified weaknesses:

> After APP 2(1) insert:
>
> Where subsection (1) does not apply, an individual must have the option of using a pseudonym unless it is impractical for an entity to deal with individuals who use a pseudonym;[22]

5.23 The exceptions to the principle are provided in APP 2(2). The OPC pointed to the provisions in APP 2(2)(a) that allowed entities not to offer an option if they are 'required or authorised by or under an Australian law, or an order of a court or tribunal, to deal with individuals who have identified themselves'. The OPC argued that as the 'authorisation is not tied to the particular circumstances', it may mean the exception is unnecessarily broad.

5.24 The OPC pointed to the case where an entity may be required to deal with identified individuals only in certain instances and not in others; for example, service delivery agencies which make payments on an identified basis, but may provide other information or services anonymously, including online. The exception under APP 2(2)(a) should only apply to the transaction if there is a legal requirement for identification for that transaction. However, the OPC argued that the wording of draft APP 2 'might be seen as exempting an entity from giving these options if it is "required or authorised" to identify individuals in any context'.[23]

5.25 The OPC put forward three options for consideration by the committee:

a. adopt the phrase 'where lawful and practicable' in APP 2, as in ALRC recommendation 20-1;
b. limit the exception in APP 2(2)(a) to where the legal requirement or authorisation applies in the circumstances of the individual's transaction; or
c. clarify and limit the breadth of the 'required or authorised by law' exception in explanatory material for this principle.

The OPC saw options A and B as being stronger than option C.[24]

5.26 Professor Greenleaf and Mr Waters put a similar view and commented that the re-wording of the exception had weakened the principle as it had moved away from NPP 8's positive formulation of 'wherever…lawful and practicable' and had

22 Professor G Greenleaf & Mr N Waters, *Submission 25*, Attachment 1, p. 3.

23 Office of the Privacy Commissioner, *Submission 39*, p. 24.

24 Office of the Privacy Commissioner, *Submission 39*, p. 25.

made it less clear that the exception applies only to those matters where identification is required by law.[25]

5.27 APP 2(2)(b) provides that if it is impracticable for an entity to deal with an individual who has not identified themselves, the entity need not provide an option of anonymity or pseudonymity. The Law Institute of Victoria (LIV) submitted that this provision is overly broad and may enable entities to circumvent APP 2(1). The isoc-au also argued that the test of 'impracticability' undermined this principle. For example, an entity may argue that it is impractical to change the information fields required for transactions online, but if that information was not reasonably necessary to the information to be provided, or the transaction to be completed, it should not have been required in the first place.[26]

5.28 In order to ensure compliance with APP 2, the LIV recommended that 'impracticable' be defined in guidance notes 'with a view to ensuring that practicability is relevant to the service or goods that the individual seeks to access'. The LIV also suggested that to improve transparency, the privacy policy of entities which wish to rely on APP 2(2)(b), and claim that it is impracticable to deal with individuals who do not identify themselves, address this issue. Alternatively, an entity should make a specific statement to individuals when personal information is sought.[27] The isoc-au recommended that APP 2 be amended so that the exemption to the principle of anonymity and pseudonymity be only allowed if the collection of personal information is reasonably necessary for one of the entity's functions or activities.[28]

5.29 Submitters noted that the ALRC recommended that the OPC provide guidance on the principle and that the Companion Guide stated that the Commissioner will be encouraged to provide guidance, 'including on the types of circumstances in which it will not be lawful or practicable to provide this option'.[29] NSW Department of Justice and Attorney General stated that:

> Guidelines on the circumstances in which compliance is to be considered impracticable under APP2 should set out matters to be considered in deciding whether compliance is practicable. They could make clear, for example, as suggested by the ALRC, that anonymity or pseudonymity generally will not be lawful in the provision of government benefits. It will be important that States are consulted on the content of any such Guidelines.[30]

---

25 Professor G Greenleaf & Mr N Waters, *Submission 25*, p. 6; see also Dr Colin Bennett, *Submission 11*, p. 2.

26 Internet Society of Australia, *Submission 41*, p. 3.

27 Law Institute Victoria, *Submission 36*, p. 4.

28 Internet Society of Australia, *Submission 41*, p. 3.

29 Australian Government, *Companion Guide, Australian Privacy Principles*, June 2010, pp 9–10.

30 NSW Department of Justice and Attorney General, *Submission 42*, p. 3.

5.30 The Department of the Prime Minister and Cabinet (the department) responded to concerns about the provision of a clear option of anonymity and pseudonymity. The department noted that the 'required or authorised' by law exception has been added into every APP. Although the ALRC report did not recommend this exception in relation to the option to interact anonymously or pseudonymously, the department commented that this 'is part of the broader policy of clarifying the operation of that exception'.

5.31 The department also commented on the concern raised by the OPC in relation to the potential for an entity relying on the lawfulness of requiring identification in one instance (for example, providing credit card information for e-commerce purposes), to require the individual to identify themselves when dealing with the entity in another instance. The department stated that 'there is nothing expressly included in the provision to broaden the scope of the exception in that way'.

5.32 The department went on to note that the ALRC examined the existing 'required or authorised by or under law' exceptions in the Privacy Act and noted generally the need for clarity about the meaning of that expression. As a result, the ALRC recommended that the OPC should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. The department concluded that 'although it is a matter for the AIC, the Department believes that the issue raised by the OPC could be included in those guidelines'.[31]

The online environment

5.33 Some submitters commented on the impact of APP 2 in the online environment. Yahoo!7 argued that APP 2 was a 'one size fits all' solution that does not recognise the diverse range of interactions taking place online and that 'context needs to dictate the appropriateness of allowing users to engage anonymously or to interact pseudonymously within these services'. In particular, Yahoo!7 raised concerns about the need to ensure that users are accountable for the use of online services. For this reason, while offering users the ability to interact with other users under a pseudonymous screen name, users are required to register and provide data so that terms of use can be enforced. Yahoo!7 also noted that this data was used by law enforcement agencies when investigating crimes that involve online services.[32]

5.34 In response to Yahoo!7's comments, the department stated it:

> …believes the use of pseudonyms is sufficient to (a) distinguish one individual from another or (b) maintain a transaction history about a person, without retaining a record of their identity. This could be used for agencies or organisations that need this information but do not need to necessarily identify an individual. In developing a framework for the protection of personal information, a key element is whether an agency or organisation

31 Department of the Prime Minister and Cabinet, *Answers to Questions on Notice*, p. 8.

32 Yahoo!7, *Submission 20*, p. 2.

> needs to collect any personal information (at all) about an individual in order to undertake its functions or interact with the individual. The standard by which agencies or organisations can determine whether personal information is needed should be based on whether it is lawful and practical to interact on an anonymous or pseudonymous basis.
>
> Therefore, if it is unlawful or impracticable for a service provider (such as Yahoo!7) to deal with individuals with anonymity or pseudonymity they would fall under the exception in APP 2(2)(a) and (b). In the cases identified by Yahoo!7 as requiring the collection of identification information (i.e. ecommerce websites authenticating identification for credit card purposes; assisting law enforcement agencies to investigate a crime; registering users for particular core services so that the terms of use of the service can be enforced), the Department's view is that these are likely to come within the exception.[33]

Conclusions

5.35 The committee considers that the provision of the option to deal with entities anonymously and pseudonymously is a positive addition to the privacy regime. However, the committee is concerned that a number of submitters were of the view that APP 2 does not provide a clear option of both anonymous and pseudonymous interactions, unless a listed exception applies; and that the provisions may be broadly interpreted so that an entity can extend the application of the 'required by law' exception inappropriately.

5.36 The committee has considered the department's response to these matters and notes the explanation provided in relation to the 'required by law' exception. However, given the concerns raised by the OPC and other submitters in relation to this exception, the committee believes that further consideration should be given to the wording of APP 2(2)(a) to ensure that the exception cannot be applied inappropriately.

Recommendation 7

5.37 The committee recommends that the wording of APP 2(2)(a) be reconsidered to ensure that the exception to the anonymity and pseudonymity principle cannot be applied inappropriately.

5.38 In relation to comments about the application of APP 2 in the online environment, the committee considers that the provision of options for dealing with entities anonymously and pseudonymously is a positive development. All too frequently it appears that unnecessary personal information is collected in the online environment. The application of these provisions will ensure that entities consider carefully their information requirements when interacting with individuals. The committee further considers that the exceptions provided in APP 2(2) provide entities with sufficient flexibility in this area.

---

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