SENATE STANDING COMMITTEE ON FINANCE AND PUBLIC ADMINISTRATION

LEGISLATION COMMITTEE

Exposure Drafts of Australian Privacy Amendment Legislation

SUBMISSION

SUBMISSION NUMBER: **39**

SUBMITTER

Office of the Privacy Commissioner

Australian Government

Office of the Privacy Commissioner

Australian Privacy Principles

Exposure Draft and Companion Guide

(June 2010)

Submission to Senate Finance and Public Administration Committee

August 2010

Table of Contents

Executive Summary

i. The Office of the Privacy Commissioner (the Office) welcomes the release of the exposure draft of the new APPs.[1] The exposure draft is the first step in implementing recommendations of the Australian Law Reform Commission's (ALRC) 2008 report, *For Your Information, Australian Privacy Law and Practice* (Report 108).[2]

ii. This submission draws on more than 20 years experience as the national privacy regulator with active involvement in the privacy law reform process. The ALRC's review of privacy was commissioned following recommendations made in the Office's 2005 Private Sector Review, and the Senate Legal and Constitutional References Committee Review, that a wider review of privacy be undertaken. [3]

iii. The Office made extensive submissions to the ALRC's review of privacy.[4] Those submissions were concerned first and foremost with ensuring that the privacy of individuals is protected and promoted now and into the future. The Office has also been consulted in the preparation of the *Enhancing National Privacy, Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (the Government Response) released in October 2009, and the draft APPs.

iv. The Office has considered the draft APPs with regard to its future role in investigating complaints, advising individuals of their privacy rights and educating agencies and organisations on their new obligations.

v. The Office welcomes the enhancements to current privacy regulation proposed in the exposure draft, consistent with the Government Response (see for example para 8). This submission focuses on areas which in the Office's view merit further consideration and improvement.

---

[1] Australian Privacy Principles – exposure draft (the APPs) viewed 19 July 2010, at www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/guide/exposure_draft.pdf; Australian Government, *Companion Guide, Australian Privacy Principles* (2010), (The Companion Guide), viewed 19 July 2010, at www.aph.gov.au/Senate/committee/fapa_ctte/priv_exp_drafts/guide/companion_guidepdf.

[2] ALRC Report 108 (2008), see www.alrc.gov.au/inquiries/privacy.

[3] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* ('Private Sector Review), March 2005, available at www.privacy.gov.au/act/review/revreport.pdf, see Recommendations 1, 5, and 69; Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988*, June 2005, see Recommendations 1 and 2.

[4] Submission to the Australian Law Reform Commission's Review of Privacy - Discussion Paper 72 (December 2007) ('Submission to DP 72'); Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 32 Credit Reporting Provisions (April 2007); Submission to the Australian Law Reform Commission's Review of Privacy - Issues Paper 31 (February 2007) ('Submission to IP 31'). Available at: www.privacy.gov.au/materials/a-z/s.

Privacy reform objectives

vi. Recognising the significant review of privacy law and practice that has occurred to date, it is important to consider whether the draft APPs meet a number of objectives that have underpinned the need for reform. In the Office's view the reform process should ensure that:

- there is a streamlined, single set of principles for the public and private sectors, which promote national consistency[5]
- privacy rights and obligations are simplified and therefore easy to understand and apply[6]
- existing privacy protections are maintained, not diminished[7]
- a high-level, principles-based, technology-neutral approach is adopted that is capable of protecting and promoting individuals' privacy into the future.[8]

Key recommendations

vii. While the draft APPs achieve the objective of a single set of principles, the Office has made a number of recommendations which it believes will further assist in meeting all the primary reform objectives outlined above. This in turn will help to ensure the effective protection of Australians' information privacy over the coming decades. These recommendations are summarised briefly below.

General issues

Greater simplicity

viii. The Office believes that the drafting of the APPs could be enhanced to make the Privacy Act more 'user-friendly for individuals, agencies and organisations', consistent with ALRC recommendations 5-2 and 18-1, and the Government responses endorsing those recommendations.[9] Some practical suggestions include:

[5] See, eg, *Enhancing National Privacy Protection, Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (2009) ('Government Response'), 'Executive Summary', pp 11 and 13.

[6] ALRC Report 108 (2008), recommendation 5-2; accepted in the Government Response (2009), p 22.

[7] Office of the Privacy Commissioner, Submission to DP72, 'Submission summary', paras 78-81; see also Government Response, p 5.

[8] See eg ALRC Report 108 (2008), recommendation 18-1; accepted in the Government Response (2009), p 37.

[9] See ALRC Report 108 (2008), recommendations 5-2 and 18-1, pp 276 and 653 respectively. See also the Government Response (2008), pp 22 and 37 respectively.

- Format the principles in the simpler style used by the ALRC in its Model Unified Privacy Principles (UPPs) or the existing NPPs.
- Use more concise language to reduce length
- Avoid repeating requirements that are substantively similar (consider grouping them in one clause)
- Consider the plain meaning of terms and use them consistently
- Keep principles high-level and generally applicable to all entities (rather than to a specific agency or organisation).

Use of 'reasonably necessary'

ix. The word 'reasonably', used throughout the draft APPs to qualify 'necessary', should be removed. The Office agrees with the Companion Guide to the APPs[10] (Companion Guide) that the issue of 'what is necessary' should be answered by reference to an objective standard. However, the Office supports the ALRC's view that 'necessary', on its own, already implies an objective test. Further, the Office suggests that a plain reading of 'reasonably necessary' may be thought to lower the existing levels of protection in the Privacy Act. This is particularly a problem in applying APP 3(1) on collection, compared with NPP 1 and IPP 1 which both use 'necessary'.

x. The Office recommends that 'reasonably necessary' be replaced with 'necessary' throughout the APPs. If required, it could be clarified in explanatory material or guidance that 'necessary' is intended to be an objective test.

Section numbering

xi. The Office also suggests consideration of the non-alignment between section numbers and the APPs, and whether alternatives such as locating the principles in a schedule to the new Privacy Act would address this problem.

Specific issues arising in the draft principles

APP 1 – open and transparent management of personal information

xii. Replace the phrase 'such steps as are reasonable in the circumstances' with the shorter expression 'reasonable steps' (as in the NPPs). This will simplify draft APPs 1, 5, 8, 11, 12 and 13 without altering their meaning.[11]

[10] Australian Government, *Companion Guide to the Australian Privacy Principles* (June 2010) (Companion Guide), p 16.

[11] See, for example, APP 1(2), APP 1(5), APP 1(6), APP 8(1), APP 11(1), APP 12(2), APP 13(5). The expression 'such steps *(if any)* as are reasonable in the circumstances' appears in APP 5(1), APP 10(1), APP 10(2), APP 12(5), APP 13(1), APP 13(3).

APP 2 – anonymity and pseudonymity

xiii. The current wording of APP 2 appears to offer a more limited right to individuals to interact anonymously or pseudonymously than the ALRC's proposed anonymity and pseudonymity principle. The Office believes the wording of the ALRC's model anonymity and pseudonymity principle could give better effect to the intended policy.[12] Alternatively, the scope of the 'required or authorised by or under law' exception to APP 2 should be clarified, so that the requirement or authorisation must apply *in the circumstances* of the individual's transaction.

APP 3 – collection of solicited personal information

xiv. Rename APP 3 'collection of personal information' and restructure to include receiving unsolicited personal information, currently dealt with separately in draft APP 4.

xv. The words 'or directly related to' could be removed from the general collection requirement in APP 3. A requirement that information be 'necessary for' a function or activity is appropriate for both agencies and organisations under a single set of principles. The inclusion of the alternative 'or directly related to' could imply that organisations may collect personal and sensitive information in a wider range of circumstances than under NPP 1. The addition of 'directly related to' was not recommended in Report 108 or the Government Response.

xvi. The segmented structure and the language of APP 3 seems complex and could be simplified. In particular, the 'necessary' collection requirement should apply to both personal and sensitive information.

xvii. Exceptions in the Privacy Act for specific agencies could be avoided. It should first be considered whether alternative means of authorising agency activities are available. This reflects the general application of the principles.

APP 4 – receiving unsolicited personal information

xviii. APP 4 could be addressed in APP 3 under a heading such as 'Receiving unsolicited personal information'. A separate, dedicated principle does not seem necessary. APP 3 is a logical place to include these requirements, and this would also reduce the number of principles.

xix. The scope and intent of APP 4 (whether or not incorporated in APP 3) could be clarified – in particular the relationship between 'collecting' and 'receiving' information.

[12] The wording of that model principle is: 'Wherever it is lawful and practicable in the circumstances agencies or organisations must give individuals the clear option of interacting by either: (a) not identifying themselves; or (b) identifying themselves with a pseudonym.' ALRC Report 108 (2008), para 20.71.

APP 5 – notification of the collection of personal information

xx. The segmented structure and the language of APP 5 could be simplified.

xxi. The term 'personal information of the kind collected by the entity' in APP 5(2)(f) could be clarified to refer to the type of information being collected at the time, as in NPP 1.3(d) and IPP 2(e). The draft clause may allow for broader and less informative notice to individuals.

APP 6 – use or disclosure of personal information

xxii. The segmented structure and the language of APP 6 could be simplified. A range of other suggestions that affect this principle are covered elsewhere (including terms like 'reasonably necessary', 'such steps as are reasonable...', 'affected individual', and additional exceptions for specific agencies).

APP 7 – direct marketing

xxiii. The draft direct marketing principle, which deals with an issue of considerable interest to the community and business, is perhaps the most complex draft APP. The principle could be re-drafted to improve simplicity and understanding, and could more clearly distinguish between individuals who have an existing relationship with an entity and those who do not.

xxiv. The ALRC's model direct marking principle, and other laws on related issues (such as the *Spam Act 2003* and the *Do Not Call Register Act 2006*) may be useful reference points for clarifying the structure and terminology of APP 7.

APP 8 – cross-border disclosure of personal information

xxv. This principle could link more explicitly with section 20 of the exposure draft, which holds entities accountable for overseas recipients' information handling in some cases. Explanatory material could also note that the principle only applies to disclosures, and not to an entity's internal 'uses' that involve overseas transfer. What constitutes a 'disclosure' in certain situations, including across computer servers, could also be further explained.

xxvi. The exception at APP 8(2)(d), for disclosures under international agreements relating to information sharing, has the potential to be broadly interpreted. It may also limit the circumstances in which an agency can be held accountable when personal information is disclosed to overseas recipients.

APP 10 – quality of personal information

xxvii. The requirement for the personal information that is used or disclosed to be 'relevant' could be linked to the purpose of use or disclosure. Otherwise it is not clear what the information should be relevant to. This would be more consistent with ALRC recommendation 27-1 and the Government's response.

APP 12 – access to personal information

xxviii. APP 12(4) proposes that agencies are required to provide access to individuals within 30 days. While no specific timeframe is proposed for organisations, it could be clarified that a 'reasonable period' for organisations to provide access would not usually be longer than 30 days.

xxix. The reference to 'the needs of the entity' in APP 12(5) could be removed, as the focus is on individual access. The phrase 'the entity must take such steps (if any) as are reasonable in the circumstances' (or the simpler, 'reasonable steps') appears to give entities sufficient flexibility to meet their needs and obligations under this APP.

APP 13 – correction of personal information

xxx. ALRC recommendation 29-5, accepted in the Government Response, proposed that personal information should be corrected if it is 'misleading', in addition to where it is inaccurate, out-of-date, incomplete or irrelevant. Overall it may be preferable to include the term 'misleading' in APP 13(1)(b)(i).

Recommendations on other issues

xxxi. The Office has no substantive, specific recommendations for APP 9 on government identifiers or APP 11 on security of personal information, beyond 'general issues' noted above.

xxxii. The provisions on extra-territorial operation of the Privacy Act could be amended to:

- clarify the scope of 'Australian link' under s 19(3)(g)
- clarify the meaning of collection of information 'in' Australia in the online context.

Office of the Privacy Commissioner

1. The Office of the Privacy Commissioner (the Office) is an independent statutory body whose purpose is to promote and protect privacy in Australia. The Office, established under the *Privacy Act 1988* (Cth) (the Privacy Act), has responsibilities for the protection of individuals' personal information that is handled by Australian and ACT Government agencies, and personal information held by all large private sector organisations, private health service providers and some small businesses.

2. From 1 November 2010, the Office of the Privacy Commissioner will be integrated into a new statutory agency, the Office of the Australian Information Commissioner (OAIC). The OAIC will bring together the functions of privacy protection (including in the private sector), freedom of information (FOI) and information policy across the Australian Government.[13] The OAIC will be the national privacy regulator of the proposed Australian Privacy Principles (APPs).

Introduction

3. The Office welcomes the release of the exposure draft of the APPs. The APPs will replace the two sets of principles in the Privacy Act that currently regulate personal information handling by Australian Government agencies (agencies) and the private sector (organisations). The new principles will therefore be a fundamental building block for streamlined, nationally consistent privacy regulation.

4. The exposure draft is the first step in implementing recommendations of the Australian Law Reform Commission's (ALRC) 2008 report, *For Your Information, Australian Privacy Law and Practice* (Report 108)[14] and the Government's privacy law reform agenda, as outlined in *Enhancing National Privacy, Australian Government First Stage Response to the Australian Law Reform Commission Report 108 (*the Government Response) released in October 2009. The final APPs will establish the foundations for the reform of Australian privacy law.

[13] Under the *Australian Information Commissioner Act 2010* (AIC Act), commencing 1 November 2010, the Office of the Privacy Commissioner will be integrated into the new Office of the Australian Information Commissioner (OAIC), which will assume the regulatory functions under the *Privacy Act 1988*. The OAIC will have 3 statutory appointees: the Australian Information Commissioner as the CEO, the Privacy Commissioner and an FOI Commissioner. With the commencement of the AIC Act, references to the Office of the Privacy Commissioner will be deemed to be to the OAIC.

[14] ALRC Report 108 (2008), see www.alrc.gov.au/inquiries/privacy.

5. In its response to ALRC Report 108, the Australian Government strongly endorsed the recommendation that the APPs should create a 'clear and simple framework for privacy obligations'.[15] The Office strongly supports this aim and has expressed its commitment to this goal in several reports and submissions.[16]

Background

6. The release of the exposure draft of the APPs in June 2010 is a significant milestone in a long process of reform:

   - In March 2005 the Office released its Review of the Private Sector Provisions of the Privacy Act (the Private Sector Review), recommending the Government consider a wider review of privacy laws in Australia.[17]
   - In June 2005 a Senate Legal and Constitutional References Committee Inquiry recommended that the Government (through the ALRC) undertake a comprehensive review of privacy regulation, including the Privacy Act.[18]
   - In January 2006 the ALRC received a reference from the then Australian Government. The ALRC's review of privacy from 2006 to 2008 included the release of Issues Papers 31 and 32, Discussion Paper 72, and extensive consultation, culminating in the release of Report 108 in August 2008.[19]
   - In October 2009 the Government announced its first stage response to Report 108, covering 197 of the 295 recommendations.[20]

7. The Office has been actively involved in the privacy law reform process since its 2005 Private Sector Review. The Office made extensive submissions to ALRC Issues Papers 31 and 32, and Discussion Paper 72; seconded staff to the

[15] Government Response (2009), p 37.

[16] See for example, Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, (2005) ('Private Sector Review'), p 8; Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Issues Paper 31*, (2007) ('Submission to ALRC IP 31'), Chapter 4; Office of the Privacy Commissioner, *Submission to the Australian Law Reform Commission's Review of Privacy – Discussion Paper 72* (2007) ('Submission to ALRC DP 72'), Proposal 15-2.

[17] Office of the Privacy Commissioner, Private Sector Review (2005), recommendation 1.

[18] Senate Legal and Constitutional References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988 (2005)*, recommendations 1 and 2. Available at www.aph.gov.au/Senate/committee/legcon_ctte/completed_inquiries/2004-07/privacy/report/index.htm.

[19] Australian Law Reform Commission ('ALRC'), Issues Paper 31, 2006, *Review of Privacy* ('ALRC IP 31'); ALRC, Issues Paper 32, 2006, *Review of Privacy—Credit Reporting Provisions* ('ALRC IP 32'); ALRC, Discussion Paper 72, 2007, *Review of Australian Privacy* (ALRC DP 72), ALRC Report 108 (2008).

[20] Government Response (2009).

Department of the Prime Minister and Cabinet (DPMC) to assist in preparing the Government Response; and has had informal input during the development of the draft APPs. The Office acknowledges the efforts of DPMC to take account of its suggestions and queries, and looks forward to further constructive engagement as the privacy law reform package develops.

8. The Office welcomes the enhancements to current privacy regulation proposed in the exposure draft, consistent with the Government Response. These include:

- the creation of a single set of principles
- re-ordering the principles to better reflect the stages of personal information flows
- the inclusion of a clear requirement for entities to consider compliance with the APPs when implementing practices, procedures and systems
- the extension of specific privacy standards for sensitive information handling by Australian Government agencies, in addition to organisations
- extended accountability of entities that disclose personal information to overseas recipients
- specific obligations for dealing with unsolicited personal information.

This submission focuses on areas which in the Office's view merit further consideration and improvement.

9. Having in mind the significant review of privacy law and practice that has occurred to date, the Office's view is that the draft APPs need to be considered in light of whether they meet a number of objectives that have underpinned the need for reform. In the Office's view, the reform process has sought to ensure that:

- there is a streamlined, single set of principles for the public and private sectors, which promote national consistency[21]
- privacy rights and obligations are simplified and therefore easy to understand and apply[22]
- existing privacy protections are maintained, not diminished[23]

[21] See, eg, *Enhancing National Privacy Protection, Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (2009) ('Government Response'), 'Executive Summary', pp 11 and 13.

[22] ALRC Report 108 (2008), recommendation 5-2; accepted in the Government Response (2009), p 22.

[23] Office of the Privacy Commissioner, Submission to DP72, 'Submission summary', paras 78-81, see also Government Response, p 5.

- a high-level, principles-based, technology-neutral approach is adopted that is capable of protecting and promoting individuals' privacy into the future.[24]

Structure of this submission

10. The Office's comments on the draft APPs are structured as follows:
    - The Executive Summary (above) notes the Office's main suggestions
    - The 'General issues' section discusses some overarching matters that the Office considers should inform the future direction of the new principles
    - 'Specific issues arising in the draft principles' outlines suggestions for improvement on each of the APPs and other parts of the exposure draft.

General issues

Simplicity

11. The Office welcomes the introduction of a single, unified set of privacy principles for the public and private sector, as proposed in the exposure draft of the APPs. A streamlined single set of privacy principles is essential to reduce undue complexity in the Commonwealth privacy regime, and the fragmentation of obligations between different industry sectors and entities.[25]

12. This submission draws on the Office's experience over 20 years in applying the Privacy Act, including the Information Privacy Principles (IPPs), and since 2001, the National Privacy Principles (NPPs).The Office has considered the APPs particularly in the context of its role as the agency that will investigate complaints under the APPs, advise individuals of their privacy rights, and educate agencies and organisations on their new obligations.

13. One of the key calls from stakeholders in the Office's 2005 Private Sector Review was for greater simplicity in the drafting of privacy protections.[26] Several stakeholders submitted that they find it difficult to fully comprehend their Privacy Act obligations, sometimes in combination with other legal regimes.[27]

[24] See eg ALRC Report 108 (2008), recommendation 18-1; accepted in the Government Response (2009), p 37.

[25] This is consistent with the Office's position in previous reports and submissions. See, eg: Office of the Privacy Commissioner, Private Sector Review (2005), p 8; Submission to ALRC IP 31 (2007), Chapter 4; Submission to ALRC DP 72, (2007), proposal 15-2.

[26] See Office of the Privacy Commissioner Private Sector Review (2005), pp 43, 201-202.

[27] See for example, Office of the Privacy Commissioner, Private Sector Review (2005), pp 42-46, 66, 68, 180, and 205.

The 2005 Private Sector Review found that greater consistency and simplicity was required to allow individuals and entities to better understand their rights and obligations under the Privacy Act.[28] In its 2007 submissions to the ALRC's privacy inquiry, the Office reiterated the need for the redrafted principles to be simple, clear and consistent.[29]

14. The Office welcomed ALRC Report 108 Recommendation 18-1:

> *The privacy principles should be drafted to pursue, as much as practicable, the following objectives:*
>
> - *the obligations... generally should be expressed as high-level principles; ...*
> - *[the] principles should be simple, clear and easy to understand and apply; ...*[30]

The Office also welcomes the Government's policy response:
'Accept: The Government strongly agrees with this recommendation.'[31]

15. The extent to which the exposure draft and APPs achieve those widely supported objectives is an important yardstick for the success of the overall reforms. However, the Office acknowledges that the combined set of principles will need to maintain a few practical differences in information handling between public and private entities.

16. Noting the views and objectives above, the Office emphasises the following factors in assessing the exposure draft and fine-tuning the APPs:

- the importance of clear and accessible language to ensure the overall effectiveness of principle-based privacy law
- the need for accessibility for individuals to understand and navigate the APPs, often without legal expertise
- the benefits of simplicity and clarity for agencies and businesses to understand and comply with their obligations (including those small businesses currently covered by the Privacy Act).[32]

[28] See for example, Office of the Privacy Commissioner, Private Sector Review (2005), pp 4-8.

[29] Office of the Privacy Commissioner, Submission to DP 72 (2007) response to Proposal 15-1. See also Office of the Privacy Commissioner, Submission to ALRC IP 31 (2007), Chapter 3, eg 3-1.

[30] The other two objectives were that the principles remain 'technology neutral' and impose 'reasonable obligations'. ALRC Report 108 (2008), recommendation 18-1, p 653.

31 Government Response (2009), Recommendation 18-1, p 37.

Principle-based law and structure – importance of accessibility and clarity

17. A key advantage of principle-based law over highly specific and technical legislation is that it can be more comprehensible to the general public, as well as those needing to apply it.[33] Agencies, all large private sector entities, and a range of existing small businesses will need to comply with the APPs.[34]

18. In the Office's view, principle-based privacy law should enable entities to understand the policy underpinning the law and to adapt their practices accordingly. The law should be clear, but also sufficiently flexible, to enable entities to determine how best to pursue their functions and activities in a way that complies with the Privacy Act.

19. Ultimately, the clearer and more easily understood such obligations are, the lower the administrative burden and cost for businesses and agencies. In addition, high levels of compliance should lead to lower levels of privacy breaches and complaints.

20. Clear and accessible language will promote public awareness and make it easier for individuals to understand and exercise their privacy rights and choices.

21. Where complaints arise, clear and comprehensible principles will also make it easier on two fronts:

    - to apply and administer the provisions (important because agencies and organisations are usually required to deal with complaints internally before an individual can complain to the Privacy Commissioner), and
    - to resolve disputes in ways that do not require specialist legal representation (important because the Privacy Act requires the Commissioner to attempt to resolve complaints through conciliation between the parties where appropriate (s 27)).[35]

[33] See for example, the discussion in Ian Turnbull QC, *Plain Language and Drafting in General Principles*, Office of the Parliamentary Counsel 1993: viewed 19 July 2010, at www.opc.gov.au/plain/pdf/plain_draftin_principles.pdf; Lisbeth Campbell, *Legal Drafting Styles: Fuzzy or Fussy?*, Murdoch University Electronic Journal of Law, Vol. 3 No. 2, July 1996, viewed 19 July 2010, at www.murdoch.edu.au/elaw/issues/v3n2/campbell.html.

[34] For example, private sector health service providers, 'reporting entities' under anti-money laundering laws, direct marketers and other traders in personal information (see ss 6D-6E of the *Privacy Act 1988).*

[35] For example, the Public Interest Advocacy Centre (PIAC), in its submission to ALRC review, advised that many clients had complained that they had been unable to understand their rights from their own reading of the Act and had been obliged to seek legal advice and representation. PIAC made the point that this is inappropriate in a jurisdiction that encourages self-representation (ALRC Report 108 (2008), para 5.68).

22. In proposing model Unified Privacy Principles (UPPs), the ALRC concluded that 'the NPPs should form the general template in drafting and structuring the UPPs', rather than following the IPPs or a completely new structure.[36] The Office notes the following passage in Report 108:

> *This proposal was widely supported [in submissions to Discussion Paper 72]. Reasons for support included that:*
>
> - *the NPPs were developed in consultation with stakeholders;*
> - *departure from the NPPs in the UPPs is likely to increase compliance costs for organisations …;*
> - *the NPPs are simpler, more concise, and more user-friendly than the IPPs; and*
> - *the ability of the NPPs to translate well into the public sector has already been demonstrated [in] Victoria, Tasmania and the Northern Territory.*[37]

Overview of suggestions for greater clarity and simplicity

23. Acknowledging the clear benefit of a single set of principles, the Office considers that the draft APPs could be phrased more simply, including when compared with the existing principles in the Privacy Act. Simpler drafting would better reflect Report 108 recommendation 18-1, some stakeholders' expectations (see para 13), and the passage quoted above. The aim in making these suggestions is to ensure the new principles are accessible, not to reduce their precision.

24. Detailed discussion of specific APPs is set out later in this submission. Some of the Office's suggestions for how specific APPs might be clarified can be categorised, in brief, as follows:

- **Format the principles in the simpler style of the ALRC's model UPPs or the existing NPPs.**
- **Use more concise language to reduce length.** For example:
  - could repeated terms be shortened ('reasonable steps' rather than 'such steps as are reasonable in the circumstances')?
  - are certain new terms needed (for example, 'individual' is more straightforward than 'affected individual'[38])?

[36] ALRC Report 108 (2008), para 18.112. The Report goes on to say 'Having drafted model UPPs… there is no need to make a specific recommendation in this regard.'

[37] ALRC Report 108 (2008), para 18.107 (footnotes omitted).

[38] While the Office understands the policy intent, a possible alternative to using 'affected individual' throughout APPs 3(3), 6(2), 8(2) and 9(2) may be to rephrase the 'serious threat' exceptions. Eg, APP 3(3)(b)(ii) could read: 'it is unreasonable or impracticable to obtain consent, from the individual to whom the information relates, to the collection' [or in other exceptions, 'to the use or

- **Avoid repeating requirements that are substantively similar.**
  For example, consider grouping these separate provisions into one clause:
    - the requirement that both 'personal information' and 'sensitive information' must only be collected where necessary for (or directly related to) the entity's functions or activities (APP 3(1) and (2))
    - the requirements for when sensitive information may be collected in APP 3(2) and (3) (compare with NPP 10)
    - obligations to notify, and the list of matters to be notified in APP 5
    - the separate rights and obligations when an individual requests to 'opt out' of direct marketing (APP 7(4) and (5))
    - options for individuals when access is refused (APP 12(5) and (9)).
- **Consider the plain meaning of terms and use them consistently.**
  For example:
    - the potentially different meaning of the term 'reasonably necessary' as enhancing or qualifying the term 'necessary' (see para 33 below).
- **Keep principles high-level and generally applicable to all entities (rather than to a specific agency or organisation).**
    - The introduction of agency-specific exceptions (such as those relating to diplomatic, consular and Defence activities) should be weighed against the increased length and complexity of the APPs, and the reduction in the principles' general applicability (see paras 71—76 below).[39]

Use of the term 'reasonably necessary'

25. The term 'reasonably necessary' is widely used in the draft APPs. The Office has a number of significant concerns regarding the use of this term in place of 'necessary'. Briefly, these concerns relate to:
    - the introduction of 'reasonably necessary' in the new collection test (APP 3(1))
    - multiple interpretations of 'reasonably necessary' in different APPs
    - varied formulations of tests relating to necessity in the exposure draft.

disclosure']. This would avoid the need to use 'affected individual' in exceptions that do not involve a 'serious threat'.

[39] Note: This is not suggesting the removal of necessary distinctions between agencies' requirements and those for organisations (see para 15).

These issues are discussed in detail below.

General collection requirements should not use 'reasonably necessary'

26. APP 3(1) sets out the proposed general requirements for collecting personal information:

> *An entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.*

The *Companion Guide to the Australian Privacy Principles* (Companion Guide) states that the term 'reasonably necessary'

> *... is intended to reflect two things. The first is that from the perspective of a reasonable person the function or activity is legitimate for that type of entity. The second is that the information collected is genuinely necessary to pursue that function or activity.*[40]

'Reasonably' appears to qualify 'necessary' rather than emphasise objectivity

27. The Office believes the draft wording of APP 3 may not give the intended effect. The word 'reasonably' could qualify 'necessary', unintentionally broadening the scope for collection and lessening the protection provided in the current IPP and NPP requirements (both of which use 'necessary').[41] The ALRC's Report 108 and the Government Response do not suggest any intention for the new collection principle to lower existing protections.[42] As the Government Response notes, 'ensuring that personal information is only collected where necessary for a function or activity of an agency or organisation is an effective measure to protect privacy.[43] The Office agrees, and considers it is vital that this standard remains clear and robust.

28. The Companion Guide also states that 'reasonably necessary' is intended to be interpreted objectively.[44] However, the ALRC's Report 108 found that it was

[40] Companion Guide (2010), p 16.

[41] IPP 1.1 requires that 'collection of the information is *necessary or directly related to*' a lawful purpose that directly relates to the agency's functions or activities. NPP 1.1 requires that 'the information is *necessary* for one or more of [the organisation's] functions or activities'. Emphasis added.

[42] See ALRC Report 108 (2008), recommendation 21-5, p 732; Government Response p 42.

[43] Government Response (2010) p 42.

[44] Companion Guide (2010), p 16.

unnecessary to provide expressly that a reasonable person's perspective applies in determining the necessity of collection:

> *The requirement in NPP 1... implies an objective test – the collection has to be necessary, not necessary merely in the opinion of the organisation. Such an interpretation is also within the spirit of the privacy principles as a whole.*[45]

29. The Office agrees that 'necessity of collection' should be an objective test. However, the Office does not agree with the Companion Guide that '*reasonably* necessary' adds a further objective requirement in draft APP 3(1), or that such a requirement is needed.

30. Under the NPPs the Office understands that 'reasonably' is used to qualify 'necessary' and provide some flexibility. For example, 'reasonably necessary' appears in NPP 2.1(h), which permits disclosures for 'law enforcement' functions.[46] In this case 'reasonably necessary' recognises that the disclosing organisation may not know with certainty what personal information will be necessary for the enforcement body's functions.

31. In the Office's view, a plain reading of 'reasonably necessary' in APP 3 could also imply a lower threshold – that collection need not be 'necessary' but only 'reasonably necessary' (which may imply the 'necessity' is less certain). The plain reading of the principle, free from any specialist legal understanding, will be important to entities trying to understand and apply the APPs. Introducing the term 'reasonably necessary' is potentially confusing and unnecessarily complex.

32. If the Committee considers that clarification is needed, one option is to make clear in the explanatory memorandum that collection of personal information must be *objectively* necessary for an entity's functions or activities, or a note to this effect in the principles. This could be supported by guidance from the Office.

Multiple meanings of 'reasonably necessary' should be avoided

33. The exposure draft appears to use the expression 'reasonably necessary' to mean different things in different principles. This problem emerges in the explanation of the particular meaning of 'reasonably necessary' in the context of APP 3(1).[47] In contrast, the term 'reasonably' appears to be intended to qualify 'necessary' when used elsewhere in the APPs, as in the existing NPP 2.1(h) (see para 30).

[45] ALRC Report 108 (2008), paras 21.75-21.78 and recommendation 21-5.

[46] NPP 2.1(h) allows disclosures by an organisation where it 'reasonably believes that the use or disclosure is reasonably necessary' for certain law enforcement activities by, or on behalf of, an enforcement body.

[47] Companion Guide (2010), p 16, quoted at para 26.

34. The Companion Guide does not provide guidance about the term where it is used in parts of the exposure draft other than APP 3(1), other than to state that the term is to be interpreted objectively and in a practical sense.[48]

35. The equivalent of NPP 2.1(h), draft APP 6(2)(e), allows an entity to use or disclose personal information without consent where:

> *the entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities by, or on behalf of, an enforcement body'* (emphasis added)

As discussed above regarding current NPP 2.1(h), this may be intended to reflect that an entity disclosing personal information for law enforcement purposes *may not know exactly what is necessary* for the enforcement body to carry out its functions or activities, so 'necessary' alone may not be appropriate.

36. The Office suggests above that 'reasonably necessary' be removed from draft APP 3(1) to minimise confusion and complexity. The Office also suggests, in the next section, that 'reasonably necessary' may not be needed elsewhere in the APPs. However, if these suggestions are not accepted, a clear and consistent meaning for 'reasonably necessary' should apply throughout the APPs.

Varied formulations of tests relating to necessity could be streamlined

37. Exceptions in the draft APPs adopt several different formulations involving the term 'necessary' (sometimes linked to 'reasonably' and sometimes linked to a 'reasonable belief'). This may be to reflect different contexts; however, it appears to result in potentially inconsistent and confusing language.

38. The Office supports distinctions that add clarity, but recommends the various tests involving 'necessary' (see below) be streamlined. An example of this is found in draft APP 3(3). This sets out exceptions to the rule that sensitive information can only be collected with consent. Similar inconsistencies arise in draft APP 6 (use or disclosure) and draft APP 8 (cross-border disclosure).

[48] Companion Guide (2010), p 16.

39. In APP 3(3), the following tests for necessity apply:

APP3(3)	Reason for collecting 'sensitive information' without consent	Necessity requirements*
APP 3 (3)(b)	To lessen or prevent a serious threat to the life, health or safety of an individual, or to public health or safety	The entity must *reasonably believe* that collection is *necessary*
APP 3 (3)(d)	The entity is a law enforcement body and the personal information relates to its functions or activities	The entity must *reasonably believe* that collection is *reasonably necessary*
APP 3 (3)(e)	For an agency's own diplomatic or consular functions or activities	The entity must *reasonably believe* that collection is *necessary*
APP 3 (3)(f)	The entity is the Defence Force and the personal information is for war, peacekeeping or aid/emergency/disaster relief activities outside Australia	The entity must *reasonably believe* that collection is *necessary*
APP 3 (3)(g)	To assist any entity to locate a missing person	The entity must *reasonably believe* that collection is *reasonably necessary*
APP 3 (3)(i)	To establish, exercise or defend a legal or equitable claim	Collection must be *reasonably necessary*
APP 3 (3)(j)	For a confidential alternative dispute resolution process.	Collection must be *reasonably necessary*

40. This table shows three different tests across seven provisions. It may be unclear to an individual, business or agency reading APP 3(3) what the various different formulations mean, which is intended to be more restrictive, and which more permissive. These three tests are considered below.

41. In APP 3(3)(d) and (g), having a 'reasonable belief' that collection is 'reasonably necessary' is understood to address two things:

- the collector's state of mind (having reasonable grounds for the belief) and
- the nature and extent of appropriate collection.

42. However, a simpler requirement that the collector must 'reasonably believe' that collection is '*necessary*' would capture both elements clearly and concisely. Adopting this wording would avoid the doubled use of 'reasonably' and could

* Emphasis added. Shading groups like terms. This table only summarises the 'necessity test' aspects of these subsections. 'Reasons for collecting' are also summaries.

reduce confusion. This wording is already proposed in the 'serious threat' exception at APP 3(3)(b).

43. In APP 3(3)(e) and (f), it is not clear why a 'reasonable belief' qualification has been introduced for the Departments of Foreign Affairs (DFAT) and the Defence Force. The Office would suggest that those agencies should be able to determine whether (rather than 'reasonably believe') the collection is 'necessary' for their *own* functions or activities, as do other agencies collecting personal information. Exceptions for specific agencies are discussed in detail below (from para 71).

44. Finally, in the exceptions for legal, equitable or dispute resolution purposes (APP 3(3)(i) and (j)), the Office considers that the phrase 'reasonably necessary' has a qualifying effect (as noted above, paras 33 to 35). Accordingly, these exceptions should adopt the term 'necessary'.

Summary

45. Overall, for clarity and simplicity the Office suggests that 'reasonably necessary' should be replaced with 'necessary' throughout the APPs. If required, the Committee could consider an alternative means of clarifying that 'necessary' is an objective test (such as in the explanatory memorandum). This change should help resolve the range of issues outlined above. This would:

- Clarify the general collection requirements in APP 3(1)
- Avoid the multiple interpretations of 'reasonably necessary' in the APPs
- Streamline the varied formulations of tests relating to necessity.

Section numbering

46. The exposure draft sets out each principle as an individual section in the Act, which do not align numerically. For example, section 2 is APP 1 and so on. The Office understands this may assist when referring to particular principles in other legislation, or where legislative amendments occur. However this may impact on the useability of the principles and make the Office's communication with parties to complaints more complex. There will be a need to refer to both a section number and a principle number, rather than just the principle. For example, 'the complainant alleges a breach of Australian Privacy Principles 3 and 5 under sections 4 and 6 of the Privacy Act...' (this example refers to section numbers in the exposure draft, noting these will change in the full Bill).

47. It could be considered whether the advantages of including the APPs in separate sections (such as 'pinpoint' referencing) outweigh the advantages of locating the APPs as Schedule 1 to the new Privacy Act (which would avoid confusion of

non-aligned sections and allow a more self-contained, 'transportable' set of principles).

Specific issues arising in the draft principles

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

48. The Office welcomes the inclusion of this principle as the first APP. The new provisions will encourage entities to manage personal information openly and transparently and to take reasonable steps to comply with the Privacy Act and handle complaints. It is important that entities understand that the 'privacy policy' requirements in draft APP 1(4) apply in addition to notification of matters under draft APP 5 when personal information is collected.

Replace 'such steps as are reasonable in the circumstances' with reasonable steps

49. APP 1 marks the draft principles' first use of the term 'such steps as are reasonable in the circumstances'. This term is used frequently throughout the APPs. The phrasing is based on the older language of the IPPs (1988). In 2001, the NPPs replaced this term with two words, 'reasonable steps'.

50. For the following reasons, the Office proposes that the APPs adopt 'reasonable steps' to replace 'such steps as are reasonable in the circumstances':

- The term 'reasonable steps' is shorter and simpler, so its adoption would reduce complexity and length of most of the APPs.
- The understanding that 'reasonable steps' has an equivalent meaning to 'such steps as are reasonable in the circumstances' can be implied from a plain reading. It can also be emphasised in explanatory material and the Office's guidance (or if necessary, a note on first use in the APPs).[49]
- Organisations are already familiar with the concept of 'reasonable steps', and agencies (currently regulated by the longer terminology) will not need to adjust their practices in moving to 'reasonable steps'.
- In some APPs, the words '(if any)' are added in cases where it may be reasonable not to take any steps, depending on the circumstances.

[49] The Office's current guidance reflects the view that reasonable steps will vary with the circumstances. See the Office's *Guidelines to the National Privacy Principles* (September 2001). For example, guidelines on NPPs 1.3 to 1.5, pp 23 and 29-32; and NPP 3 'Tip for compliance', p 43.

Using 'reasonable steps' would still enable the term '(if any)' to be included if needed.

Australian Privacy Principle 2 – anonymity and pseudonymity

51. Under draft APP 2, individuals will have the choice to use a pseudonym, as well as the choice to remain anonymous. The Office supports this principle applying to agencies and organisations. However, the exception to draft APP 2 could be interpreted as limiting the principle's application when compared to existing NPP 8 and ALRC recommendation 20-1.[50]

52. The ALRC and the Government Response both recommended that entities must provide a 'clear option' to individuals to interact anonymously or pseudonymously where it is 'lawful and practicable in the circumstances'.[51] However, APP 2(2)(a) allows entities not to offer such options 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'. Such authorisation is not tied to the particular circumstances, which may mean the exception is unnecessarily broad.

53. Many agencies and organisations are likely to have requirements or authorisations to deal with identified individuals in certain contexts and not others. For example, service delivery agencies deliver payments on an identified basis, but may offer other information or services anonymously, including online. Similarly, 'reporting entities' under anti-money laundering legislation may be required to identify customers for certain transactions, but not all.

54. In both cases, the above exception should only be available if the legal requirement or authorisation applies to the type of transaction the individual is entering (noting that another exception applies where non-identification is 'impracticable'). However, 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.

[50] ALRC Report 108 (2008), pp 706 and 708; Government Response (2009), p 39.

NPP 8 states: *Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.*

[51] ALRC Report 108 (2008), p 706; Government Response (2009), p 39.

55. To ensure the exception does not limit the ability to remain anonymous or use a pseudonym, the Office suggests three options be considered (options A and B being stronger than C):

    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.

Australian Privacy Principle 3 – collection of solicited personal information

Title and scope of APP 3

56. The Office suggests that APP 3:

    - be titled 'collection of personal information', and
    - incorporate the collection of unsolicited information (see below, para 79).

APP 3(1) – Information should be 'necessary' not 'directly related' to functions or activities

57. In developing a single set of principles, some existing requirements in the IPPs and NPPs have needed to be reconciled. APP 3 combines aspects of the collection requirements under IPP 1 and NPP 1. Draft APP 3(1) requires that personal information must be 'reasonably necessary for, or directly related to' the entity's functions or activities in order to collect it.

58. The Office suggests ALRC recommendation 21-5 gives a simpler alternative, reflecting the basic structure of NPP 1:

    The 'Collection' principle... should provide that an agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.[52]

    The Government Response agreed, noting among other things that '"Necessary" should be interpreted objectively and in a practical sense'.[53]

[52] See ALRC Report 108 (2008), recommendation 21-5. See also *Privacy Act 1988* (Cth) Sch 3, NPP 1.1.

[53] Government Response (2009), p 42.

59. In line with the ALRC recommendation and the Government Response, the Office believes the phrase 'necessary for one or more of the entity's functions or activities' is sufficient for all entities under a single set of principles.

60. Retaining the 'directly related' alternative in the APPs is unnecessary for agencies, and appears to lower the existing NPP standard for organisations, including when collecting sensitive information.[54]

61. The suggestion to limit collection to what is 'necessary' is not intended to restrict agencies' existing ability to carry out their functions or activities. IPP 1 currently authorises agencies to collect personal information where it is necessary for, or directly related to, a lawful purpose that is directly related to a function or activity of the agency.[55] As agencies' functions and activities are often tied to enabling legislation, objects clauses or related instruments, they are often more easily defined than for organisations. The Office is not aware of examples where the 'necessary' requirement would prevent an agency from collecting personal information to pursue legitimate functions or activities.

62. On the other hand, organisations' functions and activities are rarely established by legislation. The Office is concerned that expanding the options for organisations to what is 'reasonably necessary for, or directly related to' their functions or activities could introduce uncertainty. For example, APP 3 could be interpreted as allowing a broader range of personal information to be collected than under NPP 1. This potentially broader scope would also apply to collection of sensitive information (see APP 3(2)(a)(i)), which is usually ascribed higher levels of protection than other information.[56] This could be inconsistent with the intent to enhance, not diminish, privacy protections.[57]

63. To improve certainty, simplicity and effectiveness of the collection principle, the current level of protection in NPP 1 should be maintained by removing the words 'or directly related to' from APP 3(1) and corresponding provisions. Agencies' existing collection of personal information would continue on the basis that the information is 'necessary' for those functions or activities. This would also reflect the ALRC's recommendation and the Government Response.

Structure of APP 3 should be simplified

64. The Office suggests that the structure of the collection principle could be simplified.

[54] See *Privacy Act 1988* (Cth) Sch 3, NPP 1.1; see also draft APP 3(1) and (2)(a)(i).

[55] *Privacy Act 1988* (Cth) s 14(1).

[56] See, eg, Privacy Act, Schedule 3, NPP 2.1(a) and NPP 10.

[57] See Government Response (2009), p 5.

65. Under the Privacy Act, 'sensitive information' is a subset of 'personal information'. The general rule of 'necessary collection' that applies to personal information should also be the starting point for sensitive information. However, draft APP 3(1) separates and excludes sensitive information from this general rule. The rule is then replicated for sensitive information at APP 3(2)(a)(i), but only in combination with a consent test.

66. To simplify the structure of APP 3, the Office suggests:

- removing the exception 'other than sensitive information' from APP 3(1)
- deleting APP 3(2)(a)(i), which would then be redundant
- consolidating the exceptions to permit the collection of sensitive information (subclause (3)) as a simpler 'list' under APP 3(2), as in NPP 10 and the ALRC's model UPP 2.5.[58]

67. The Office understands that draft APP 3(2) intends to give primacy to the 'consent' exception by separating it from the other exceptions in subclause (3). However, as there is no requirement to consider whether consent is possible first, the practical benefit of separating the exceptions appears limited, and the resulting structure and wording may be unduly complex.

Collecting sensitive information should be 'necessary' not 'directly related'

68. APP 3(2) states that entities must not collect sensitive information unless:

- 'the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; and
- 'the individual consents to the collection...;' *or*
- one of the exceptions in APP 3(3) applies.

This 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. This lowers the existing threshold of NPP 1, which requires that information is 'necessary' for a function or activity, and applies to all personal information including sensitive information.[59]

[58] ALRC Report 108 (2008), p 733.

[59] The Office understands that the current higher requirements for collecting sensitive information in NPP 10 apply *in addition to* NPP 1. If NPP 10 obligations replaced those in NPP 1, rather than being 'additional', then other NPP 1 obligations such as notice may not apply to sensitive information, which would be contrary to the spirit of the Act.

69. 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.

70. The Office's proposed changes to APP 3 above should resolve several issues regarding the collection of sensitive information. In summary those changes would:

- remove the words 'or directly related to' from APP 3(1) and corresponding provisions
- remove the exception 'other than sensitive information' from APP 3(1), so that *any* personal information must be 'necessary' for a function or activity to be collected (but not 'reasonably necessary')
- remove APP 3(2)(a)(i), as it would be redundant
- consolidate the additional exceptions for collecting sensitive information (now in APP 3(3)) under APP 3(2).

'Exceptions' for agency-specific activities – alternative options could be considered

71. A number of the APPs include new exceptions for a range of diplomatic, consular and Defence Force activities.[60] These first appear in APP 3(3)(e) and APP 3(3)(f), which set out exceptions to the general rule that sensitive information should only be collected with consent. The APPs are intended to provide a broad framework for the appropriate collection, use or disclosure of personal information by both agencies and organisations. The principles take account of agencies' specific personal information handling activities in a range of ways, including through the 'required or authorised by or under law' exceptions. It is the Office's view that it is preferable that specific activities are addressed in portfolio legislation or elsewhere, so that these Privacy Act exceptions come into play where appropriate. Other general exceptions may also apply in some circumstances, such as for threats to life or safety, for law enforcement, or public revenue protection.

72. Keeping the Privacy Act's exceptions generally applicable will maximise the APPs' coherence and relevance to all entities. This is consistent with the recommended objectives that the principles should be 'high-level', and should be redrafted to achieve greater logical consistency, simplicity and clarity.[61]

[60] See for example, APP 3(3)(e), APP 3(3)(f), APP 6(2)(f), APP 8(2)(h), APP 8(2)(i).

[61] ALRC Report 108 (2008), recommendations 18-1 and 5–2 (both accepted in the Government Response, pp 37 and 22).

73. Before additional and more specific exceptions are introduced into the Privacy Act, all available alternatives should be fully explored. It is important that agencies are aware of the existing flexibility for their operations under the IPP framework, as well as the proposed changes to those exceptions following Report 108 and the Government Response. For example:

- New exceptions are proposed in the APPs in relation to missing persons; and for serious threats to life, health or safety of an individual (following the removal of the 'imminence' test[62]), or to public health or safety.[63]
- Part VIA of the Privacy Act will continue under the new regime, clarifying that information exchanges may occur between certain entities in declared emergencies and disasters (such as the 2009 Black Saturday bushfires).[64]
- There will also be scope to seek a Public Interest Determination from the Privacy Commissioner (as there is now) to suspend one or more principles where activities in the public interest would breach the APPs.

74. The Office could also provide advice and guidance on how agencies can undertake their functions in compliance with these existing and proposed provisions.

75. The inclusion of broadly worded exceptions to the general principles could also reduce agencies' accountability for their activities, in ways the community may not expect. For example, APP 3(3)(e), as currently drafted appears broad. The term 'diplomatic or consular functions or activities' could cover a very wide range of activities. As proposed, an individual may not be able to dispute the handling of personal information which met those broad exceptions.

76. The Office recognises that it is not always possible for agencies to address these matters in portfolio legislation, nor will a Public Interest Determination necessarily be the most efficient way to address integral aspects of an agency's ongoing functions. The inclusion of agency-specific exceptions in the Privacy Act should be limited to situations where there is no appropriate alternative. It could also be considered whether any such exceptions could be accompanied by rules made by the Privacy Commissioner in accordance with s 21 of the exposure draft, as with the 'missing persons' exceptions (APPs 3(3)(g)(ii) and 6(2)(g)(ii)).

[62] Existing exceptions for use and disclosure, such as NPP 2.1(e) and IPP 11.1(c), require that such a threat be both 'serious' and 'imminent'. However ALRC Report 108 recommended, and the Government Response accepted, that the 'imminent' test be removed. This will permit a slightly wider range of disclosures.

[63] See, for example, draft APP 3(3)(g) and APP 3(3)(b) respectively.

[64] See Companion Guide, p 6.

77. Overall, any such exceptions, or authorisations in other legislation, should balance the agencies' needs to fulfil their functions, with individuals' expectations of personal information protection and agency accountability.

APP 3(3) 'necessity requirements'

78. The various formulations of requirements for necessity in the exceptions under APP 3(3), and the use of the term 'reasonably necessary' in APP 3(1), are discussed above, at paras 37 to 44.

Australian Privacy Principle 4 – receiving unsolicited personal information

APP 4 could be combined with APP 3 (collection)

79. The Office suggests that the receipt of unsolicited information should be addressed under a subheading 'Receiving unsolicited personal information' within the general collection principle at APP 3, rather than in a separate, dedicated principle. The Office understands that the receipt of unsolicited information may not be intended to involve 'collection' as defined by section 15 of the exposure draft (see next para). However, it is suggested that the general collection principle is nevertheless the logical location for a provision relating to unsolicited information. If the Office's suggestions to simplify the structure of APP 3 outlined above were implemented, addressing unsolicited personal information in APP 3 would maintain this principle at a reasonable length and reduce the overall number of principles.

Clarify relationship between collecting and receiving

80. The Office suggests that a note or explanatory guidance should clarify that, in the context of APP 4(4), a technical 'collection' will not be a breach of APP 3 (such as for unnecessary collection), if the 'collected' information was:

- unsolicited, but then
- dealt with appropriately in line with APP 4.

This appears to be the intent of APP 3(6), but this connection may not be obvious.[65]

[65] Draft APP 3(6) states that 'This principle [APP 3] applies to the collection of personal information that is solicited by an entity.'

Australian Privacy Principle 5 – notification of the collection of personal information

Structure

81. As with the collection principle, the Office suggests that the notification principle (draft APP 5) could be shortened and made easier to understand, by:

- making APP 5(1) into a shorter, single provision, and
- including APP 5(2) within APP 5(1) – reflecting the existing, simpler structure of NPP 1.3 and IPP 2.

82. The Office suggests that the term 'as is reasonable in the circumstances' is unnecessarily repeated in APP 5(1)(a) as this is already stated in the introduction at APP 5(1).

83. The Office also questions whether the separate clauses (1)(a) and (b) are needed. These require entities (a) 'to notify...' or (b) 'to otherwise ensure that the individual is aware of...'. The existing NPP 1.3 uses 'reasonable steps to ensure the individual is aware of', which seems adequate and simpler. The principle's title could still refer to 'notification' without a separate reference in (1)(a).[66]

APP 5(2)(f) – usual disclosures

84. This clause requires entities to notify individuals to whom the entity 'usually discloses personal information of the kind collected by the entity'. This requirement seems less specific than advising individuals about usual disclosures of 'information of *that* kind' (meaning the kind collected) in the NPPs.[67] This link is also explicit in IPP 2, where the equivalent clause states that the notice should relate to 'information of the kind *so* collected'.[68]

85. The Office suggests the APP should refer to the kind of information actually being collected, as in the NPPs and IPPs. The current draft provision may be interpreted to mean notice must be given about the kind of information the entity collects *more generally*. Such notice may be lengthier and less relevant to the individual's case, especially where an entity collects different types of

[66] For illustrative purposes, draft APP 5(1) and (2) could instead read as a single clause, eg: '*At or before the time an entity collects personal information about an individual (or if that time is not practicable, as soon as practicable after collection), the entity must take reasonable steps to [notify the individual or otherwise] ensure that the individual is aware of: (a) the identity and contact details of the entity; ...*

[67] *Privacy Act 1988* (Cth), Schedule 3, NPP 1.3(d), emphasis added.

[68] *Privacy Act 1988 (Cth)*, s 14, IPP 2(e), emphasis added.

personal information and discloses it in a variety of ways. A broader overview of the entity's practices may be more suited to privacy policies under APP 1.

Australian Privacy Principle 6 – use or disclosure of personal information

Structure

86. The Office suggests that APP 6(1) and (2) could be made into a shorter, single provision. The proposed cross-referencing structure and wording of APP 6(1)(b) and 6(2) may also make the principle more difficult to understand. The Office suggests that the list of exceptions (in subclause (2)) to the general rule that consent is required before using or disclosing for a secondary purpose (in subclause (1)(a)) could be merged into a single list within APP 6(1).

Agency-specific exceptions

87. Draft APP 6(2)(f) would allow an agency (currently DFAT) to disclose personal information without consent for diplomatic and consular functions and activities. The Office's general views on agency-specific exceptions in the Privacy Act is set out in relation to APP 3 (collection), from para 71 above.

Varied formulations of tests relating to necessity

88. The exceptions listed at APP 6(2) contain various formulations of necessity requirements and uses of the term 'reasonably necessary'. The Office's comments on these issues are outlined above ('Key issues', from para 37).

Australian Privacy Principle 7 – direct marketing

89. The handling of personal information for direct marketing is an area of concern for many individuals, as the ALRC Report 108, the Government Response and the Office's Community Attitudes Surveys suggest.[69] If direct marketing is to be addressed in a separate principle, it is important that the principle be clearly drafted, easily understood, and proportionate with community expectations.

[69] ALRC Report 108 (2008), pp 890-891; Wallis Consulting Group, *Community Attitudes Towards Privacy 2007*, prepared for the Office of the Privacy Commissioner (2007), p 29.

Improving the direct marketing principle's structure

90. In the Office's view, the ALRC's model direct marketing principle, UPP 6, would provide a good starting point for the structure of APP 7,[70] notwithstanding the policy differences outlined in the Government Response.

91. The current structure may make it difficult to interpret and apply the principle, as the reader is directed to various subsections within it. The Office suggests that cross-referencing be kept to a minimum and clauses be combined where there are commonalities.

92. The principle's structure could be simplified and reorganised to reflect the general rules that regulate how information can be used or disclosed for direct marketing, followed by exceptions (such as for contracted service providers) and any additional requirements.

93. There are other ways the principle's length could be reduced. For example, the introductory phrase in APP 7(1), 'If an organisation holds personal information about an individual', could be removed. The phrase appears redundant, as an organisation could not use or disclose personal information if it doesn't 'hold' the information.[71]

Clarify terminology and structure for 'existing' and 'other' customers

94. The Government accepted, with amendment, ALRC recommendation 26-1. The Government Response supported a separate direct marketing principle which distinguishes between direct marketing to 'existing customers' (or those with an 'established relationship') and to individuals 'who are not existing customers'.[72] This corresponds to model UPP 6. Noting that 'customer' might not best characterise the relationship in all contexts, the Government undertook to seek advice from the Office of Parliamentary Counsel on how to reflect a broad meaning of 'customer'.[73]

95. Accordingly, the Companion Guide states that 'the language used in the drafting of this principle differs to that outlined in the Government response to

[70] See ALRC Report 108 (2008), Volume 1, p 97.

[71] The Office understands that the principle is intended to apply whether 'direct marketing' is the primary purpose or a secondary purpose of collection, so presumably that is not the reason for the phrase.

[72] ALRC Report 108 (2008), p 898.

[73] Government Response (2009), p 56.

the ALRC report..., but achieves the same policy.'[74] Part of the intent is to apply more stringent obligations when using personal information of non-existing customers as the individual is less likely to expect use or disclosure for direct marketing purposes.

96. The Companion Guide states that the policy for 'existing customers' is applied to 'individuals who have provided personal information to the entity who is undertaking the direct marketing'. The policy for 'non-existing customers' is applied to 'those who have not provided personal information to the entity who is undertaking the direct marketing'.[75]

97. However, the principle itself appears more complex than this, as there are exceptions to the above approaches that depend on individuals' reasonable expectations for use and disclosure. The Office suggests that the language in the principle could more clearly distinguish between individuals who have an established relationship with an organisation and those who do not.

98. The ALRC explained that the concept of an 'existing customer' should require 'some kind of ongoing commercial, contractual or business relationship'.[76] The ALRC Report suggests that a one-off purchase would not usually be sufficient to suggest an ongoing commercial, contractual or business relationship.[77]

99. The ALRC report noted that the concept of an ongoing or pre-existing relationship is used in other regimes that regulate direct marketing, such as the *Spam Act 2003*, the *Do Not Call Register Act 2006* and the Australian Direct Marketing Association's (ADMA) *Direct Marketing Code of Practice*.[78] The Office suggests considering whether consistent terms could be adopted from those Acts or codes. This may help to ensure that:

- APP obligations are well understood across the industry and smoothly incorporated within existing compliance frameworks, and
- individuals can readily understand their rights, and marketers' obligations.

100. The Office acknowledges the Government's concerns regarding the use of the term 'customers', but suggests that this could be resolved either by:

- defining the term in the principle or the definitions clause (s 15), or

[74] Companion Guide (2010), p 11.

[75] Companion Guide (2010), p 11.

[76] ALRC Report 108 (2008), p 911.

[77] ALRC Report 108 (2008), p 911.

[78] See ALRC Report 108, pp 907-911; Australian Direct Marketing Association, *Direct Marketing Code of Practice* (2006), p 8.

- using the concept of ongoing or existing relationships.

APP 7(3) – 'Personal information collected from another person etc'

101. Despite its subheading, draft APP 7(3) includes provisions that apply where the information is collected from:

- *the individual*, where 'the individual would not reasonably expect the organisation to use or disclose the information for that purpose;'
- as well as 'from a person other than the individual...' (further conditions apply).

102. While more substantive changes are needed, the current subheadings in draft APP 7(2) and (3) could better reflect their intent and contents. For example (respectively, with emphasis added):

- *Personal information collected from individuals with an established relationship*
- *Personal information collected about individuals without an established relationship*

Opt-out requirements could be simplified

103. The wording of APP 7(4) and APP 7(5) could be reworded to make it easier for organisations and individuals to understand what should happen if an individual requests to 'opt out' of marketing, or wants to know where their personal information was sourced.

104. The 'opt-out' provisions in draft APP 7(4) and APP 7(5) could be simplified along the lines set out in the ALRC's model UPP 6.3.[79] As the model principle suggests, it seems redundant to include APP 7(4), which states that an individual 'may request' not to receive further direct marketing communications. Instead, this right can be implied by setting out the organisation's obligations if an individual *makes* such a request – as at APP 7(5).

105. The Office suggests a more compact clause could replace and combine relevant parts of APP 7(4) and (5). This could reduce repeated wording and cross-referencing. Similar to UPP 6.3, the replacement clause could state that, if an individual requests an organisation to cease the use or disclosure of the individual's personal information for direct marketing, or for facilitating direct marketing by other organisations, then the organisation:

[79] See ALRC Report 108 (2008), Volume 1, p 97, for this UPP.

- must not charge the individual for the making of, or to give effect to, the request; and
- must give effect to the request within a reasonable period after the request is made.

106. Another combined clause could replace draft APP(4)(c) and 5(c) on information sources. This could state that, if an individual asks the organisation to provide the source of (or where it collected) the individual's personal information used for direct marketing purposes, the organisation must, within a reasonable period of the request, notify the individual of the organisation's source, unless it is impracticable or unreasonable to do so.

Application of the principle to agencies' commercial activities could be clarified

107. The ALRC recommended that the direct marketing principle apply to organisations only. It suggested that in their commercial activities, agencies should adopt best practice by meeting the requirements of organisations under the direct marketing principle.[80] Agencies' non-commercial activities would be regulated by the general use and disclosure principle. The Government Response appeared to go further, stating that 'where agencies are engaged in commercial activities, they should be required to comply' with the principles, which would include for direct marketing.[81] If this is the intended effect of the draft note to APP 7(1), this is unclear from the note itself.[82] The note could better reflect the position outlined in the Government Response.

Australian Privacy Principle 8 – cross-border disclosure of personal information

Add a note on accountability

108. The Office suggests that a note be inserted under draft APP 8(1) to the effect that, unless an exception in APP 8(2) applies, section 20 will hold the entity accountable for activities of the recipient which would breach the APPs. Section 20 will not apply if the APPs apply to the recipient directly (draft s 20(1)(c)).

[80] ALRC Report 108 (2008), para 26.48. See also its recommendations 26-1 and 26-2.

[81] See Government Response to recommendation 26-1, p 56; and the Companion Guide, p 6; which also refer to the effect of s 7A of the Privacy Act.

[82] The proposed note to draft APP 7(1) states: 'An act or practice of an agency may be treated as an act or practice of an organisation.'

Scope of the principle – 'disclosure' not 'use', and related bodies corporate

109. While APP 8 explicitly adopts the term 'disclosure', rather than 'transfer' which is used in NPP 9, explanatory material could note that APP 8 (and related provisions[83]) would not apply to the overseas movement of personal information if that movement is an internal 'use' by the entity, rather than a 'disclosure'.[84]

110. Explanatory material could also clarify that APP 8 *will* apply where an organisation sends personal information to a 'related body corporate' located outside of Australia. The ALRC's Report 108 proposed changes to s 13B of the Privacy Act to clarify that the 'cross-border' principle will apply to such disclosures (accepted in the Government Response).[85]

Routing of personal information outside Australia

111. The Companion Guide indicates that it is not intended that a 'disclosure' will occur when personal information is routed through servers that may be outside Australia.[86] The Office agrees with this view provided the personal information is not accessed by a third party during this process. The Companion Guide or other explanatory material could note that entities will need to take a risk management approach to ensure that personal information routed overseas is not accessed by third parties. If the information *is* accessed by third parties, this will be a disclosure subject to APP 8 (among other principles).

APP 8(2)(d) – international agreements

112. APP 8 proposes an exception for agencies where Australia is party to an international agreement relating to information sharing, and the disclosure is required or authorised under this agreement. The scope of this exception is unclear to the Office. As an exception to APP 8(1), it may limit the circumstances in which an agency can be held accountable when it discloses personal information overseas.

[83] Other clauses that refer to the disclosure of personal information to overseas recipients include APP 1(4)(g) (openness and transparency), APP 5(2)(j) (notification), and the note under APP 6(1) (use or disclosure).

[84] The Companion Guide does not discuss this, although 'Disclosure vs Transfer' is discussed, p 12.

[85] ALRC Report 108 (2008), Recommendation 31-5: 'Section 13B of the Privacy Act should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia or an external territory, the transfer will be subject to the 'Cross-border Data Flows' principle.' Accepted in the Government Response (2009), p 79.

[86] Companion Guide (2010), p 12.

113. The Office reiterates its view that agency disclosures of personal information out of Australia should be done by way of the 'required or authorised by or under law' provision. Wherever practicable, specific domestic legislative authority should be the basis for an agency to disclose personal information under an international agreement relating to information sharing.[87] This would provide clarity and certainty to agencies where portfolio legislation or other laws allow disclosures overseas. It would also ensure that agencies' information sharing activities are subject to sufficient parliamentary scrutiny.

114. Where there is no specific legislative authority to disclose personal information that is the subject of a particular international agreement, the Office's view is that the exchange of information should be subject to other scrutiny, such as through a public interest determination (a legislative instrument) issued by the Privacy Commissioner.[88] These alternative options may be preferable to a separate and potentially broad exception for 'international agreement[s] relating to information sharing'.

115. In considering the rationale and effect of this proposed exception, the Committee may wish to:

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

APP 8(2)(g) – disclosing to overseas bodies 'similar' to Australian enforcement bodies

116. The Office understands that APP 8(2)(g) is intended to apply where an agency discloses information to an overseas recipient where this is necessary for law enforcement activities by, or on behalf of, an Australian enforcement body. The requirement for the overseas recipient to be 'a body that performs functions, or exercises powers, that are *similar* to those performed or exercised by an enforcement body' (emphasis added) could be broadly interpreted.

117. As 'enforcement body' is strictly defined for the Australian context in s 15, the Office suggests limiting disclosures under this clause to overseas recipients that

[87] See Office of the Privacy Commissioner submission to ALRC DP 72 (2007), response to ALRC Proposal 28-3, pp 393-397.

[88] See, eg, Temporary Public Interest Determination No 2010-1 (to allow collation of victims of crime statistics involving student visa holders for research purposes), 5 May 2010, at: www.privacy.gov.au/materials/types/determinations/view/7081.

perform functions or exercise powers that are *substantially similar* to those of an Australian enforcement body. The term 'substantially similar' is used in the context of transborder data flows under NPP 9(a) and in draft APP 8(2)(a)(i), referring to information handling regimes in other countries.

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

118. APP 8 sets out exceptions allowing cross border disclosure for diplomatic, consular and some Defence Force activities, without taking steps to ensure that the overseas recipient does not breach the APPs (APP 8(2)(h) and (i)). The Office's general position on agency-specific exceptions is outlined under APP 3 (paras 71–76).

119. The relationship between these exceptions to APP 8, and the general policy intent that agencies' overseas activities will be covered by the APPs, is unclear. The Office notes that, independent of these exceptions, acts or practices that are 'required by an applicable law of a foreign country' will continue to be authorised.[89]

Australian Privacy Principle 9 — adoption, use or disclosure of government related identifiers

120. The Office considers that the added coverage of state and territory-issued identifiers in draft APP 9 is an appropriate step and may facilitate further national consistency in personal information handling.

121. Draft APP 9 adopts the term 'reasonably necessary' under exceptions to the general rule that organisations should not use or adopt government identifiers (APP 9(2)(a), (b) and (f)). For the Office's views on this see 'Use of the term '"reasonably necessary"' (under 'General issues', para 25 above).

122. The Office suggests that in APP 9(2)(a) and (b), the entity proposing to use or disclose an identifier should be in a position to determine what is objectively necessary for the permitted purposes, so the word 'necessary' would be more appropriate. In APP 9(2)(f), both 'reasonably believes' and 'reasonably necessary' are used. As in other instances, the latter phrase could simply be 'necessary'.

[89] See Companion Guide, pp 7 and 12. That is, 'The policy achieved by subsection 6A(4) and section 13D of the existing Privacy Act will be replicated in the new Privacy Act' for agencies and organisations (Companion Guide, p 7).

Australian Privacy Principle 10 – quality of personal information

123. APP 10(2) requires 'such steps (if any) as are reasonable in the circumstances' to ensure that personal information that is used or disclosed is accurate, up-to-date, complete and relevant. The Office suggests that the 'relevance' requirement should be linked to the purpose of use or disclosure. As drafted, it is not clear what the information should be relevant to.

124. Linking relevance to the purpose may give better effect to the policy intent of ALRC recommendation 27-1 and the Government Response, which stated:

> *Agencies and organisations should take reasonable steps to make certain that the personal information they collect, use or disclose is, with reference to the purposes of that collection, use or disclosure, accurate, complete, up-to-date and relevant.*[90]

Australian Privacy Principle 11 – security of personal information

125. The Office has no substantive issues to raise with the Committee regarding the security principle.

Australian Privacy Principle 12 – access to personal information

APP 12(5) —'Other means of access'

126. Draft APP 12(5) provides that where an entity refuses access, or refuses to give access in the manner requested:

> *the entity must take such steps (if any) as are reasonable in the circumstances to give access to the information in a way that meets the needs of the entity and the individual.*

127. The Office believes the reference to 'the needs of the entity' in APP 12(5) should be removed, as the focus is on individual access. The phrase 'the entity must take such steps (if any) as are reasonable in the circumstances' (or the simpler, 'reasonable steps') gives entities sufficient flexibility to meet their needs and obligations under this APP.

[90] Government Response (2009), p 61 (emphasis added).

128. APP 12(5)(a) could be removed. APP 12(5) begins:

> *(5) If:*
>
> *(a) an individual requests an entity to give access to personal information about the individual; and*
>
> *(b) the entity refuses…*

129. As APP 12(5)(b) refers to refusing access under relevant provisions, APP 12(5)(a) seems redundant. Removing this clause would reflect the simpler structure of NPP 6.3 and the general structure of ALRC model UPP 9 (see, eg, UPP 9.8: 'Where an agency or organisation denies a request for access…').

130. APP 12(9)(a) also seems redundant and could be removed for similar reasons.

Evaluative information exception

131. APP 12(3)(j) allows organisations not to give an individual access to the extent that access would reveal evaluative information generated within the entity in connection with a commercially sensitive decision-making process. The Office believes that individuals should retain the same rights under this provision as provided by its equivalent, NPP 6.2.

132. Where NPP 6.2 applies, an organisation 'may give the individual an explanation for the commercially sensitive decision rather than direct access to the information'. APP 12(3)(j) provides a similar exception for organisations not to give access where this would reveal evaluative information. However, there is no specific equivalent in APP 12 for 'explanations' to be given for the decision (for example, in relation to insurance cover or denial of credit). It may be intended that existing rights be given effect by way of APP 12(5) – access 'in a way that meets the needs of... the individual'; and (9) – written reasons for refusal.[91] This could be clarified however, to ensure a right to be given reasons for a decision is preserved (not just a reason for refusing access).

Timeframe for requests for access

133. APP 12(4)(a) distinguishes between agencies and organisations by expressly identifying that agencies are to respond to a request for access within 30 days after the request is made.

[91] ALRC Report 108 suggested that, consistent with NPP 6.2, the Access and Correction principle should allow for entities to provide an explanation for the commercially sensitive decision where they rely on this type of exception. The ALRC also recommended including a note to the effect that the mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under this exception. (See ALRC Report 108 (2008), p 1020.)

134. The Office suggests APP 12(4)(a) as currently drafted may unintentionally imply that a reasonable period for *organisations* to provide access may be longer than 30 days. While NPP 6 does not set out timeframes for providing access, guidance produced by this Office suggests that access should be granted within 14 days if granting access is straightforward, or within 30 days if granting access is more complicated.[92] It is suggested that a note under APP 12(4)(a) could clarify that a reasonable period for organisations to provide access will not usually exceed 30 days.

Australian Privacy Principle 13 – correction of personal information

APP 13(1)(b)(i) – no reference to correction where personal information is misleading

135. APP 13(1)(b)(i) does not include any reference to correcting personal information that is 'misleading'. ALRC recommendation 29-5, which was accepted in the Government Response, proposed that personal information should also be corrected if it is 'misleading' (in addition to where it is inaccurate, out-of-date, incomplete or irrelevant). IPP 7(1)(b) refers to correcting information that is 'misleading', although NPP 6.5 does not.

136. Overall it may be preferable to include the term 'misleading'. The Office notes that the proposed definition of 'personal information' (s 15) still includes 'an opinion', and the term 'whether true or not' now applies to both 'information' and 'opinions'.

137. For example, a factual statement about a person being convicted of a crime is likely to be misleading if it fails to note that the person's conviction was subsequently quashed.

Extra-territorial application of the new Privacy Act

138. Section 19(2) of the exposure draft applies the Privacy Act to acts and practices done outside Australia, by organisations that have an 'Australian link'. Section 19(3)(g) states that an organisation has an Australian link if:

> *both of the following apply:*
>
> *(i) the organisation carries on business in Australia;*

[92] Office of the Privacy Commissioner, *Guidelines to the National Privacy Principles* (2001), p 49.

(ii) the organisation collects or holds personal information in Australia whether before or at the time the act is done or the practice is engaged in. (emphasis added)

Clarifying the scope of 'Australian link' under s 19(3)(g)

139. The existing equivalent to s 19(3)(g) above is s 5B(3) of the Privacy Act. That existing provision states that an organisation has an 'Australian link' if:

- '...(b) the organisation carries on business in Australia...' and
- '(c) the personal information was collected or held by the organisation in Australia... either before or at the time of the act or practice.'

The difference in referring to 'the' personal information appears significant. It applies the test of 'Australian link' to *the personal information involved in a particular overseas act or practice* of the organisation, to determine whether the Privacy Act will apply to that act or practice.

140. By comparison, draft s 19(3)(g)(ii) establishes an Australian link if 'the organisation collects or holds personal information in Australia'. As it refers to 'personal information' generally, it does not appear to require that 'the' specific item of personal information that is involved in a particular overseas act or practice was collected or held in Australia. This may unintentionally imply that, once an organisation collects or holds *any* personal information in Australia, an individual located overseas could complain under the Privacy Act about the organisation's acts or practices outside Australia, in relation to any personal information the organisation holds about the individual (even if *that information* was never collected or held in Australia).

141. Accordingly, the Office recommends that the scope of the Privacy Act's extra-territorial operation be clarified along the lines of existing s 5B(3). For example, the Act could require that 'the personal information' involved in an organisation's overseas act or practice was collected or held in Australia in order for the Act to apply to that act or practice.

Clarifying the collection of information 'in' Australia in the online context

142. There can be some uncertainty as to how s 5B of the Privacy Act applies to personal information submitted online by individuals in Australia to an overseas-based organisation. The issue is whether the collection occurred 'in' Australia or not. For example, it might be argued that the collection occurred *outside* Australia if collected via the internet from a person in Australia.

143. Given that the internet has allowed greater transfer of personal information across national boundaries, clarifying the scope of extra-territorial operation of the Privacy Act would enhance the Office's ability to apply the Act in these circumstances. The exposure draft's changes to s 5B (see para 138), do not clarify the issue of where online collection occurs.

144. Accordingly, it could be clarified in s 19(3) that the Privacy Act applies to overseas acts or practices where the personal information is collected *from* or held in Australia. This may help to clarify that the Act applies where personal information is collected via the internet from an individual who is physically in Australia. There may also be alternative ways to clarify that personal information 'collected or held in Australia' includes such information collected over the internet.