Cyberspace Law and Policy Centre
A Centre for the Public Interest in Networked Transactions

Strengthening uniform privacy principles: an analysis of the ALRC's proposed principles

Submission to the Australian Law Reform Commission
on the Review of Australian Privacy Law Discussion Paper 72

Graham Greenleaf, Nigel Waters & Lee Bygrave

Graham Greenleaf
Professor of Law
University of New South Wales

Nigel Waters
Principal Researcher, Interpreting Privacy Principles Project
Cyberspace Law & Policy Centre, UNSW Faculty of Law

Lee Bygrave
Associate Professor, Department of Private Law
University of Oslo
Visiting Fellow, Faculty of Law, University of New South Wales

Research Assistance

Abi Paramaguru, Research Assistant on the *Interpreting Privacy Principles Project*

17 December 2007

Research for this submission is part of the Interpreting Privacy Principles Project, an Australian Research Council Discovery Project

INTERPRETING PRIVACY PRINCIPLES

Strengthening uniform privacy principles: an analysis of the ALRC's proposed principles

Contents

Introduction

Structure of Submission

This submission responds to Part D of the Australian Law Reform Commission's Discussion Paper 72 Review of Australian Privacy Law, September 2007 which deal with the information privacy principles lying at the heart of the *Privacy Act* 1988 (renamed 'Unified Privacy Principles' (UPPs) by the ALRC), and the definitions which are essential to their meaning.

We will make separate submissions on the promotion and enforcement of the principles, on exemptions, on credit reporting, and on some other aspects of DP 72.

Background – the iPP Project

Research for this submission has been undertaken as part of a Discovery project funded by the Australian Research Council, 'Interpreting Privacy Principles'. The home page for the project, and other publications relating to the project, are at <http://www.cyberlawcentre.org/ipp/>. The *iPP Project* is based at the Cyberspace Law & Policy Centre at UNSW Law Faculty. The principal objective of this research is to conduct over the course of the project (2006-09) a comprehensive Australian study of (i) the interpretation of information privacy principles (IPPs) and 'core concepts' in Australia's various privacy laws, particularly by Courts, Tribunals and privacy regulators; (ii) the extent of current statutory uniformity between jurisdictions and types of laws, and (iii) proposals for reforms to obtain better uniformity, certainty, and protection of privacy.

Concerning the first element, a small but rapidly growing body of cases has developed in Australia over the last few years. Around a hundred Tribunal decisions, a similar quantity of mediated complaint summaries, and relatively small number of relevant Court decisions have become available. There has been little systematic analysis of this material. The relative scarcity of Australian interpretative materials means that the objective necessitates consideration of the interpretation of similar IPPs and core concepts in the privacy laws of other Asia-Pacific countries (particularly New Zealand, which has the largest quantity of reported cases) and European jurisdictions. The iPP Project, as it develops this analysis, will aim to make further inputs into the ALRC's review and similar privacy reform projects at State level.

1. Key Terminology

At the outset, we comment on the definitions which are essential to the interpretation of the UPPs.

1.1. Personal Information

The ALRC proposes a number of changes relating to the definition of personal information (DP72, Proposal 3-5):

> *(a) The Act should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.*
>
> *(b) The Explanatory Memorandum of the amending legislation should make clear that an individual is 'reasonably identifiable' when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.*
>
> *(c) The Office of the Privacy Commissioner should provide guidance on the meaning of 'identified or reasonably identifiable'.*

We support Proposal 3-5 (a) to make the definition more consistent with international terminology.

The ALRC considers that 'the collection of information about internet users with the intention of linking that information to names and addresses; and targeting individuals with advertising without linking the information to names and addresses or making any effort to identify individuals in the physical world' should be within the meaning of 'personal information' (DP72, [3.136]). The ALRC notes that the Privacy Commissioner is also of this view, and no doubt the guidance proposed in (c) could clarify this.

We support the definition of personal data being strengthened or clarified to ensure that it does cover those situations where information is sufficient to allow either interaction with persons on an individualised basis, or the imparting of consequences on an individualised basis, as proposed by the Australian Privacy Foundation in its previous submission, and by the authors in previous articles and submissions. It does not matter whether such interactions or consequences are beneficial or detrimental to the individual: what makes the data 'personal information' is that the individual is treated differently from other individuals because of information which is specific to them, even though their name may not be known to the party which is using the information. We also note that the European Union (EU) 'Article 29' Committee also seems to consider that 'personal data' under the EU privacy Directive can have such a meaning (see Opinion 4/2007 on the concept of personal data, at p14).

However, we are not convinced that either the existing or the proposed definition of 'personal information' would necessarily be interpreted this way by an Australian court, in which case any guidance under Proposal 3–5 (c) would be to no avail (see our generic comments on OPC guidance in our submission on Part F of DP72). We

suggest there should be specific legislative clarification, as this question is essential to the future operation of privacy legislation in relation to emerging technologies with increasingly broad impact such as radio frequency identification device (RFID), digital rights management (DRM) and geo-location technologies.

The ALRC considers that information 'that simply allows an individual to be contacted' without conveying anything about the individual's identity or characteristics should not and would not be within the proposed definition of 'personal information' (DP72, [3.139]). We agree with this, but consider that it also needs to be addressed in any legislative clarification.

> ***Submission DP72-1: The definition of 'personal information', or the explanatory memorandum in relation thereto, should state that it covers those situations where information is sufficient to allow interaction with persons on an individualised basis, or the imparting of consequences on an individualised basis. This should not include information which merely allows an individual to be contacted without conveying anything about the individual's identity or characteristics.***

1.2. Sensitive information

The ALRC proposes that the definition of 'sensitive information' in the *Privacy Act* should be amended to include: (a) biometric information collected for the purpose of automated biometric authentication or identification; and (b) biometric template information (DP72, Proposal 3-6).

We support Proposal 3–6.

The question of genetic samples is directly relevant to the ALRC's current privacy review, and we suggest that the ALRC should now revisit the privacy issues concerning genetic samples, contrary to its position that it will not do so, (DP72, [6.77]). That position was reasonable prior to the November 2007 federal election, given that the previous government had not accepted the ALRC's earlier recommendations, but the new government should now be given the opportunity to reconsider the matter.

> ***Submission DP72-2: The ALRC should re-visit the question of genetic samples in the context of this review.***

The ALRC has considered our earlier submission that information about an individual's financial affairs should be included in the definition of 'sensitive information', but has concluded that it should not (DP72, [3.168]).

We agree with the ALRC's reasoning and conclusion concerning financial information.

The ALRC proposes that the definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual prferences and practices (DP72, Proposal 3-7)

We support Proposal 3.7

1.3. Record

The ALRC proposes that the definition of 'record' should be amended to include both a document and information stored in electronic or other forms (DP72, Proposal 3-8).

We agree with the ALRC's intention in Proposal 3–8, but suggest that there may also be need to clarify that 'a person' cannot constitute an 'other form' of storage of information. A person should not be a 'record' of their own biometric data, and nor should a person be regarded as 'storage' of everything that they know. The latter possibility would defeat the purpose of the general restriction of the Act's operation to personal information stored in records, excluding information only 'stored' in a person's mind (as considered in *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192).

> ***Submission DP72-3: We support Proposal 3–8 but submit that if it is adopted, there will need to be a corresponding clarification that 'a person' is not an 'other form' of storage.***

1.4. Generally available publication

The ALRC proposes that the definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication (DP72, Proposal 3-9).

We support Proposal 3–9.

Other definitions

See below (Section 3) for our comments on the meaning of 'consent'.

In our submissions on specific UPPs, we sometimes recommend that other terms be clarified – and we indicate where we believe this could best be achieved by a statutory definition.

2. Structural Reform of the Privacy Principles

In chapter 15 of DP72, the ALRC addresses broader reform issues relating to the Privacy Principles.

2.1. Level of Detail, Guidance and Protection

The ALRC proposes that the privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives: (a) the obligations in the privacy principles generally should be expressed as high level principles; (b) the privacy principles should be simple, clear and easy to understand and apply; and (c) the privacy principles should impose reasonable obligations on agencies and organizations (DP72, Proposal 15-1).

We support Proposal 15-1. However we believe that it is also desirable to adopt principles (i) which are consistent, at least within Australia, and (ii) which represent best practice in internationally accepted privacy standards (CLPC IP31, Submission 4-36).

2.2. Single Set of Privacy Principles

The ALRC proposes that the *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles—the Unified Privacy Principles (UPPs)—that would be generally applicable to agencies and organisations, subject to such exceptions as required (DP72, Proposal 15-2).

We support Proposal 15-2. However, we suggest that the ALRC should consider the name 'Uniform Privacy Principles', because 'unified' refers to the fragmented past, whereas 'uniform' describes the substantive result of the process of unification. If adopted, 'unified' would be a puzzle to future 'users' of the law, whereas 'uniform' would convey a more important message.

> ***Submission DP72-4: The proposed new set of privacy principles should be known as the Uniform Privacy Principles***

The ALRC proposes that UPPs should apply to information privacy except to the extent that:(a) the *Privacy Act* or another piece of Commonwealth primary legislation imposes different or more specific requirements in a particular context; or (b) subordinate legislation under the *Privacy Act* imposes different or more specific requirements in a particular context (DP72, Proposal 15-3).

We support this proposal, but only to the extent that such differences or greater detail are justified. If it is possible for the UPPs to cover a situation, it is desirable that they do so. Even where differences of substance or detail are justified on some specific points, it is generally desirable for the UPPs to apply, and for a separate specific provision to provide the amending difference or detail. This will maximise the consistent application of interpretations by Courts and tribunals.

2.3. Scope and Structure of UPPs

The ALRC proposes that the National Privacy Principles should provide the general template in drafting and structuring the proposed UPPs (DP72, Proposal 15-3).

We support Proposal 15-3.

3. Consent

In Chapter 16 of DP72, the ALRC explores the issue of consent asking (a) whether the definition of consent should be amended; (b) whether the OPC should issue further guidance on the meaning of consent; and (c) should the proposed UPPs contain a separate principle that deals with the issue of consent (DP72, [16.2]).

3.1. A Separate Privacy Principle Dealing with Consent?

The ALRC is of the view that it would be inappropriate to deal with consent as a discrete privacy principle (DP72, [16.43]). We agree with this.

The ALRC is also of the view that 'the most pressing problem in relation to consent is not its status within other privacy principles but rather its meaning in the Act and what agencies and organisations should do in order to obtain consent' (DP72, [16.47]). The ALRC believes that this problem can best be rectified by providing greater guidance as to the meaning of 'consent' and how this applies in particular contexts. For the reasons outlined below, while we support such guidance being given, we consider that this would be inadequate on its own, and that definitions are also required.

3.2. Meaning of Consent

The ALRC believes that there are 'four critical factors' that apply when considering whether an individual consents to the handling of his or her personal information in a given situation (DP72, [16.25]):

- The context in which the consent is sought.
- Whether there is informed consent.
- Whether the consent is voluntary.
- Whether the individual's option to consent to one purpose is freely available and not bundled with other purposes.

The ALRC proposes that the Office of the Privacy Commissioner should provide further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should (a) cover consent as it applies in various contexts; and (b) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent' (DP72, Proposal 16-1).

In our view, this proposal by the ALRC does not go far enough to rectify the problems associated with understanding consent. As outlined below, we do not have sufficient confidence in the OPC issuing guidelines in a timely manner, or in such guidelines being followed satisfactorily.

The ALRC suggests that if it becomes apparent that the OPC's guidance is not being heeded or that the consent exceptions in the privacy principles are being relied upon inappropriately, then further legislative action may be warranted (suggesting primary or subordinate legislation to specify what is required to obtain consent in the relevant field of activity) (DP72, [16.35]). The clear history of abuse in the area by agencies and organisations warrants the implementation of such legislative action earlier rather

than later. It is unlikely that there will be a second round of well-considered privacy reforms in the short or medium term.

> ***Submission DP72-5:The definition of 'consent' should be amended to deal with a number of key issues concerning consent, specified in the following submissions, rather than leaving them to OPC guidance. Other aspects of consent should be dealt with where possible in the Explanatory Memorandum, and only otherwise by OPC guidance.***
>
> ***Submission DP72-6: Whether or not our submission DP72-5 is accepted, we submit that the OPC should be required to issue guidelines on a specified list of issues concerning consent within one year.***

Implied consent

The *Privacy Act 1988* and *Information Privacy Act 2000 (Vic)(IPA)* define 'consent' as including express consent or implied consent (PA s.6 IPA s.3). In relation to international standards, the EU Directive requires that 'the data subject has unambiguously given his consent' (Art. 7(a)) as one of the bases for any processing of personal data. Insofar as any implied consent is also unambiguous, IPPs 10–11 and NPP 2 are compatible with the standard adopted in the EU Directive, provided they are interpreted as requiring free and informed consent.

> ***Submission DP72-7: In relation to implied consent, either the definition of 'consent' or the explanatory memorandum should state that implied consent must be clear and not ambiguous.***

The ALRC notes the OPC's position that implied consent can be inferred from an individual's 'failure to opt out provided that the option to opt out was clearly and prominently presented and easy to take up' (DP72, [16.4]), but does not comment further. We consider that it is wrong and dangerous for *mere* failure to opt out to ever be regarded as consent, and inconsistent with the ALRC's view that consent 'necessarily implies an element of voluntariness; otherwise the concept is indistinguishable from passive acceptance'. Failure to opt out can be relevant to consent being implied, such as where a person goes ahead in the face of a clear opt-out notice and provides information where they genuinely have a choice not to provide it, but it should always involve some further positive act. For example, if a person has already provided personal information, but is only then presented with an opt-out notice concerning additional uses of the information, that is not consent. In support of our position, we draw attention to the decision of Justice Nicholson in *Australian Communications and Media Authority v Clarity 1 Pty Ltd* (2006) 150 FCR 494 – a *Spam Act* 2003 cited by the ALRC in relation to telecommunications privacy (DP72, [64.77]).

It is obviously not sufficient to leave it to the OPC to set guidelines on this issue, as their previous approach has been manifestly inadequate on this point.

> ***Submission DP72-8: Either the Act or the Explanatory Memorandum should state that a failure to opt out is not by itself to constitute consent.***

Consent vs acknowledgement of conditions

Many data users seek 'consent' for uses and disclosures in circumstances where individuals are required to consent in order to proceed with the transaction or receive the service. This is from one perspective not 'free' consent, but from another the individual is free not to go ahead with the transaction. Privacy Commissioners have issued advice that in these circumstances data users should not pretend that they are seeking consent, but should instead ask the individual to simply acknowledge that the uses and disclosures specified will take place and are a condition of the transaction.[1]

Whilst more 'honest', acknowledgement alone might not then be a sufficient basis for the use or disclosure (other than under the IPPs – which have a 'prior notice' exception discussed below). One of the other exceptions to the use and disclosure principle would have to apply. The credit reporting provisions of the *Privacy Act* (Part IIIA) refer expressly to consent in relation to transactions where individuals do not have any choice, other than not to proceed with their application for credit.

> ***Submission DP72-9: The ALRC should give further consideration to the implications of the confusion caused by the lack of any distinction in the Privacy Act between uses or disclosures justified by consent and those justified by acknowledgment of notification. At the least, the Act or the Explanatory Memorandum should state that where a person has no choice but to provide personal information in order to obtain a benefit, no consent to any uses of the information beyond the express purpose of collection may be implied. In such circumstances of 'involuntary consent', only express consent should apply.***

Bundled consent

Bundled consent means the practice of seeking consent for multiple uses and/or disclosures at the same time (OPC, 2005, p. 85) – typically when collecting personal information. Individuals are given no choice as to the particular uses or disclosures to which they are consenting, or not consenting – it is in effect 'all or nothing'. The issue of bundled consent has been well canvassed by the Privacy Commissioner. Bundled consent exposes a major flaw in the practical efficacy of the principles in meeting the objective of participation by individuals.

Organisations employ this practice of 'bundled consent' for reasons of efficiency and cost reduction. The ALRC notes the argument that costs to obtain consent for each use would be passed on to the consumers (DP72, [16.7]), but this point is true of all regulatory compliance. The practice of 'bundled consent' undermines the interests served by the consent requirements of the *Privacy Act*. Yet the Act currently gives some leeway for the practice due to the reference in NPP 1.3(c) to a plurality of purposes and the omission of guidance as to the meaning of 'primary purpose' in NPP 2.1. Where secondary uses or disclosures are necessarily incidental to the primary purpose e.g. disclosure to a mailing contractor for delivery, or to another agency for verification of details provided, then it may be appropriate to make this a condition of

[1] See for instance Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles*, edition.02, September 2006, KC 52, p.17.

a transaction. But too often, data users seek consent for secondary uses which are neither necessary for nor even necessarily related to the primary purpose – most commonly for marketing other goods or services, but also for more significant and potentially even more unwelcome purposes. We discuss these issues further in our comments on UPP 5.

While there might be limited situations where bundled consent is tolerable, the ALRC has too readily accepted that bundled consent is appropriate in certain circumstances (DP72, [16.25]).

In its 2005 private sector review report, the OPC noted that there is a need to clarify the limits for bundling consent under the Act. The OPC states that it will 'develop guidance' on the issue (OPC (2005), recommendation 22, p. 93), but this has yet to appear. What needs to be made clearer is the extent to which data users are allowed to rely on consent obtained in this way and conversely, the extent to which individuals must be given separate opportunities to consent to different uses/disclosures.

One method of reducing abuse of the leeways mentioned above in relation to 'specific notification' and 'use and disclosure' principles would be to require separate consents for each purpose, where consent is required.

> ***Submission DP72-10: The definition of 'consent' needs to be amended in order to prevent abuse of the practice of 'bundled consent'. In particular, wherever consent is applicable to the operation of a privacy principle, separate consent should be required for each proposed purpose of use.***

4. Anonymity and Pseudonymity (UPP 1)

4.1. Introduction

The ALRC proposes that the anonymity principle would be expanded to explicitly allow identification by a pseudonym, where its use would not be misleading. Government agencies, and not only the private sector as at present, would have to allow individuals to deal with them on an anonymous basis where this would be lawful and practicable.

ALRC proposed UPP 1

> *Wherever it is lawful and practicable, individuals, when transacting with an agency or organisation, should have the clear option of either:*
>
> *(a) not identifying themselves; or*
>
> *(b) identifying themselves with a pseudonym, provided this would not be misleading.*

We draw attention to our submission on biometric technology in response to DP72 Part B, which is highly relevant to this principle.

4.2. Expansion of Anonymity Principle

We support both the placement of this principle first in the UPPs, and the extension of this principle to agencies (CLPC IP31, Submission 4-30). We also support the extension of this principle to expressly include pseudonymity (CLPC IP31, Submission 4-29 and Submission 4-29.1).

The ALRC proposal retains the words '… individuals … should have …', in contrast with the stronger Northern Territory *Information Act* formulation that '… organisation[s] must give individuals …'. This is inconsistent with all other UPPs, and does not make it unambiguous that organisations and agencies are obliged to provide this option.

> ***Submission DP72-11: UPP 1 should state that 'agencies and organisations must give individuals the option of anonymity/pseudonymity, not that 'individuals … should have' this option. (This reformulation is also necessary in relation to our next submission).***

4.3. The Option to Transact Anonymously or Pseudonymously

We support the refinement that the option to transact pseudonymously should be 'clear', rather than 'explicit' or 'express' (DP72, [17.32]).

Although it notes that use of the word 'clear' would 'allow' compliance with UPP 1 through systems design (DP72, [17.32]), the ALRC does not discuss requiring anonymity and pseudonymity options to be 'designed in' to information systems (see further, e.g., Bygrave, 2002, p. 371). It will be all too easy for data users to argue that it is impracticable to offer these options once design decisions have been made that preclude them. This is particularly likely given the ALRC's acceptance that the requirement of 'practicability' includes that UPP 1 will not apply if providing the

option will place an unreasonable financial burden on the organisation or agency (DP72, [17.18]).

An obvious example is cashless toll roads, where the opportunity for anonymous travel has been removed by the removal of cash booths and the choice of tolling systems and business models that require vehicles (and their registered owners) to be identified. Had sufficient attention been paid to an anonymity/pseudonymity principle at the outset, it should have been possible to design automated toll roads that either respected the right of anonymous travel (through the use of pre-paid debit tags) or at least offered 'pseudonymous' accounts where identification of the actual user would only be triggered by exceptional events, (such as non-payment, accidents or crime). The need for this principle to be incorporated in systems design also exposes one of the weaknesses of the complaints-based model of enforcement – complaints that toll roads in Australia do not comply with NPP 8 are pointless because the operators can legitimately argue that it is 'too late' and now impracticable. The principle can only effectively be enforced by a pro-active regulator anticipating the compliance issue and intervening at the design stage of information systems.

> ***Submission DP72-12: UPP 1 should expressly state that the obligation on organisations/agencies applies at the stage when an information system is being designed, not only 'after the event' when a person wishes to enter a transaction with a data user. This is to mean that where it is practicable, without excessive cost, to design anonymity/pseudonymity options into a system, they must be designed in. The judgements as to practicability and as to whether any cost is excessive must not be left to the organisation/agency – they must be able to be tested by an independent party.***

Another enhancement of the anonymity principle would be to make it clear that the obligation extended to facilitating anonymous transactions with third parties (CLPC IP 31, Submission 4-29). As an example, a representative complaint under the *Privacy Act 1988* about charging for 'silent' telephone lines (unlisted numbers) failed because a telco itself needs to identify its subscribers (both for billing and as a statutory requirement)[2]. If NPP 8 required telcos to facilitate the ability for subscribers to remain anonymous in their interaction with third parties then it would be possible to argue that charging for silent lines breached the principle.

> ***Submission DP72-13: The anonymity principle should impose an obligation on organisations to facilitate, where practicable and lawful, anonymous or pseudonymous transactions between individuals and third parties***

The ALRC suggests that one example of where it may be unlawful or impracticable to offer anonymity/pseudonymity is where an individual may intend to act fraudulently (DP72, [17.18] bullet 2 and [17.22]). This is not a good example and, if reflected in either the principle or in guidance, would leave the door open for organisations/agencies to argue that this was always the case. It is impossible to know in advance the motives of an individual in seeking anonymity or using a pseudonym. Any system can and will be abused in isolated cases – and that alone is not sufficient justification for exemption from this principle. It would only be reasonable to decline

---

[2] See http://www.privacy.org.au/Papers/Silent-Line-v5.rtf

to provide anonymous or pseudonymous option where an overall assessment of the resulting risk of fraud or other unlawful behaviour was both high and widespread – i.e., where it was likely to be abused by many individuals.

The inclusion of the 'not misleading' element in the proposed UPP1 is unnecessary and inoperable. The whole point of a pseudonym can be seen as being to deliberately mislead (at least the casual observer, but in some cases even the recipient) as to identity. The example given by the ALRC of a person using another individual's name (DP72, [17.23]) is not a good one – in most transactional contexts this would be fraudulent (where there was an intention to impersonate), while in some contexts it could be harmless and unobjectionable (such as using a celebrity's name in fun). In any case, it is not practical to place an obligation on organisations/agencies that depends on knowledge of individuals' intentions. The qualification 'where lawful and practicable' should cover all the necessary exceptions.

> ***Submission DP72-14: The words '..,provided this is not misleading' should be deleted from paragraph (b) of UPP1.***

In summary, the effect of our submissions would be revised wording for UPP 1 as follows:

> ***Submission DP72-15: UPP 1 should read: "An agency or organisation must, where lawful and practicable, give individuals the option of either:***
>
> ***(a) not identifying themselves; or***
>
> ***(b) identifying themselves with a pseudonym***
>
> ***This obligation applies both in the operation of an information system and at the stage when a system is being designed, and should include facilitation of anonymous or pseudonymous transactions between individuals and any third parties for whose use the system is designed."***

5. Collection (UPP 2)

5.1. Introduction

ALRC proposed UPP 2

2.1 An agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.

2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

2.3 If it is reasonable and practicable to do so, an agency or organisation must collect personal information about an individual only from that individual.

2.4 If an agency or organisation collects personal information about an individual from the individual or from someone else, it must comply with UPP 3.

2.5 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either: (a) destroy the information immediately without using or disclosing it; or (b) comply with all relevant provisions in the UPPs that apply to the information in question, as if the agency or organisation had actively collected the information.

2.6 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required or specifically authorised by or under law; or

(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent; or

(d) if the information is collected in the course of the activities of a nonprofit organisation that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims—the following conditions are satisfied:

(i) the information relates solely to the members of the organisation or to individuals who have regular contact with it in connection with its activities; and

(ii) at or before the time of collecting the information, the organisation undertakes to the individual whom the information concerns that the organisation will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

5.2. Collection from the Individual

We support the ALRC's proposed extension to agencies of the requirement to collect personal information, 'where reasonable and practicable' directly from the data subject (DP72, Proposal 18-1(a)).

We also support the ALRC proposal that the OPC should provide further guidance to clarify when it would not be reasonable and practicable to collect personal information directly from the individual (DP72, Proposal 18-1(b)), subject to our general comments about OPC guidance in our submission on DP72 Part F.

5.3. Unsolicited Personal Information

In our previous submission (CLPC IP 31, Submission 4-4) we supported the application of the 'Collection' principle to unsolicited information.

The ALRC proposes that when information about a person is collected from a third party, the collector would have the choice of destroying the information (without using or disclosing it) or complying with the privacy principles as if it had directly collected the information from the person to whom it relates. This would include giving notice to the person. The law is currently unclear on this. (DP72, Proposal 18-2 and UPP 2.5).

We support this qualified application of the collection principle to unsolicited information, provided it is made clear that 'using or disclosing' includes taking *any* action, and that the destruction option must be exercised within a very limited time – otherwise it would be essential for at least the security principle to apply while the information was held.

However, we consider that, although the better view is that the NPPs do apply to unsolicited information, this is not beyond doubt (see Greenleaf 2001). If a Court interpreted the collection principle so as not to include unsolicited information within the meaning of 'collect' then this could have disastrous consequences for the scope of the legislation and in particular the collection principle, as may be the case in NSW as a result of *WJ v Commissioner for Fair Trading* [2007] NSWADT 11. It is therefore desirable that the Act or Explanatory Memorandum make it clear that unsolicited information is included, independently of the merits of the ALRC's Proposal 18-2.

> ***Submission DP72-16: The Act or Explanatory Memorandum should make it clear that unsolicited information is included within the meaning of 'collect'.We comment further below on other means of collection.***

5.4. Limitation on collection – reasonable purposes

Most privacy laws share a common requirement that collection of personal information be lawful, necessary, relevant and 'minimal'[3], but there are significant differences in the precise wording, and consequently the meaning, of each of these component requirements. In our previous submission (CLPC IP 31, Submission p. 15) we noted that the Issues Paper did not enquire into this aspect of collection principles[4] and yet it is fundamental to the concepts of purpose specification (an express element of the OECD Guidelines) and proportionality (an implicit element underlying all sets of privacy principles).

---

[3] Expressed variously as 'relevant and not unreasonably intrusive' (PA IPP 3(c) & (d)) and PPIPA s11(a) & (b); and 'adequate but not excessive in relation to that purpose' (HK DPO DPP 1(1)(c)).

[4] There is only a passing reference in paragraph 4.15.

We consider the approach in the Discussion Paper is inadequate in that it only takes up one aspect of this issue.

The ALRC proposes only a 'reasonable belief of necessity' test within UPP 2 (DP72, Proposal 18-3 and UPP 2.1). While we support the inclusion of this additional test, we believe that overall the obligation remains too subjective, and that further guidance is desirable within the principle itself concerning several of the other criteria. We make the following suggestions:

Purpose justification

Further to our previous submission (CLPC IP 31, Submission 4-5.1) we favour a version of the test used in some Canadian privacy laws, as noted by the ALRC in paragraph 18.41 and now supported by the OPC (DP72, [18.40]). The concept of proportionality is also central to all European developments in privacy jurisprudence, particularly in the European Court of Human Rights, and its incorporation into Australian information privacy law would be of assistance in enabling Australian courts to make use of this continually developing jurisprudence, and would help align Australian law with international standards.

The test needs to go to the reasonableness of the purpose rather than merely the reasonableness of information collection in the context of whatever function or activity the organisation/agency specifies

> ***Submission DP72-17: Add to UPP 2.1 the words '…and is proportional to those functions or activities'.***

Excessive collection

The proposed UPP 2.1 retains the wording of NPP 1 '…necessary for one or more of its functions or activities', without any express linkage to the particular purpose of collection of that information. This leaves it open to an agency or organisation to argue after the event that they have not breached the collection principle because they can demonstrate a connection to one of their purposes even though it is clear that the collection of the information in question was for another purpose.

The collection obligations should expressly link the amount of personal data that may be collected to the purpose of collection, and limit it to what is necessary for that purpose.

> ***Submission DP72-18: Add to UPP 2.1 a second sentence: 'The perceived necessity must be related to the particular purpose of collection of the information in question.'.***

Lawful purpose(s)

The proposed UPP2.1 shares another weakness of NPP 1.1 in that it only requires collection by a private sector organisation to be 'necessary for one of more of its purposes'. The reference to 'purposes' could imply '*lawful* purposes', but we believe this should be made explicit as it is in IPP1, PPIPA s.8 and HKDPO DPP 1(1). The law should make it clear that collection can only be for a lawful purpose.

As we have said previously (CLPC IP 31, Submission 4-5.1), this does not mean that there would need to be express legal authority for the collection. In common law jurisdictions any action that is not unlawful is, by default, lawful. Our proposed wording will generally only operate as a negative condition preventing collection of personal information to further an unlawful purpose.

Submission DP72-19: UPP 2.1 should refer to 'one or more of its lawful functions or activities.'. .

5.5. Sensitive information

The ALRC proposes to include the substantive content of NPP10 into the new collection UPP (2.6), where it will apply to both organisations and agencies (DP72, Chapters 18 & 19). We support this in principle, but have some reservations concerning the exceptions.

We note that the ALRC has not taken up the recommendation from the OPC to require express/explicit consent, preferring to rely on generic guidance on the meaning of consent (discussed in Chapter 16). As we have noted in relation to that chapter we do not think it sufficient to rely on guidance alone to address potential abuse of consent exceptions, and this is particularly true in relation to sensitive information.

Submission DP72-20: The consent exception in UPP 2.6(a) should require express or explicit consent.

The proposed exception for collection that is required or specifically authorised by law (b) is broader than the existing 'required by law' exception in NPP10. We comment on the more general application of this distinction in relation to Chapters 13 & 22, but support the inclusion of 'specifically authorised' in UPP 2.6(b).

Submission DP72-21: The exception (b) in UPP 2.6 should include the word 'specifically'.

The exception for emergency situations (c) is also proposed to align with the equivalent use and disclosure exception, i.e. to apply where there is a 'serious threat…' without the additional requirement (currently found in NPPs) that the threat be 'imminent'. For the reasons we give in relation to UPP 5, we oppose the deletion of the qualifying word 'imminent' in UPP 2.6 (c).

Submission DP72-22: We oppose the deletion of the word 'imminent' from UPP 2.6(c)

The ALRC asks if provision should be made for collection of sensitive information without consent in connection with the provision of essential services (DP72, Question 19-1). While we appreciate the potential benefit to some individuals in special circumstances of such an exception, we also point to the potential for it to be abused – many well meaning agencies and organisations will in our experience understandably take advantage of any provision which avoids extra hurdles in their work, but could easily do so either where consent could and should be obtained (albeit with some effort) and where the consequences of the collection may not necessarily be perceived by all affected individuals as beneficial.

Our answer to Q 19-1 is therefore no.

The final exception (d) to UPP 2.6 relates to non-profit organisations with specified aims While there is no specific explanation, this appears to be a combination of the existing equivalent NPP10.1(d) and the definition in that exception of 'non-profit organisation', without any substantive change in effect. We take this opportunity to note that the definition seems oddly worded in several respects e.g. 'trade' aims are arguably too broad an objective for a trade association, and 'racial' aims sounds very negative. We suggest a preferable alternative that refers directly to the definition of sensitive information in the Act, and adds the caveat that the activities must be lawful, to avoid the exception covering organisations unlawful discrimination, race hate etc (while the two conditions should also have this effect, it would be better for the exception to make this point more clearly).

> ***Submission DP72-23: The first paragraph of UPP 2.6(d) should read 'if the information is collected in the course of the lawful activities of a non-profit organisation that has aims relating to sensitive information (as defined in this Act) – the following conditions are satisfied:'***

We note that the issue of an exception to this and other principles for research use is discussed in Part H and will provide our comments on that more general issue in our separate submission.

Use and disclosure of sensitive information

While we agree that it makes sense to include provisions relating to the collection of sensitive information within a general collection principle, it exposes more clearly the lack of any additional obligations in relation to the use and disclosure of sensitive information (other than in a limited way in proposed UPP 5.1(a)). As the ALRC notes (DP72, [19.19]) having a separate principle (NPP 10) has arguably given the misleading impression that it covered more than just collection issues. We disagree with the ALRC view that 'the most dangerous risks with respect to sensitive information are [best] dealt with at the initial stage of collection' (DP72, [19.34]). We address this issue further in the context of the Use and Disclosure UPP.

5.6. Other Aspects of the 'Collection' Principle

Means of collection

The proposed UPP 2.2 adopts the wording of NPP 1.2 and applies it to both organisations and agencies.

The ALRC has not, in DP72, addressed the issues of lawfulness and fairness which we raised previously (CLPC IP 31, Submission 4-5.7). We repeat our arguments:

Lawfulness of means of collection - Means of collection can be unlawful because of a breach either of criminal law or of civil law requirements (such as by trespass, inducing breach of contract etc). A government agency acting *ultra vires* in collecting information beyond the scope of express collection powers would be another basis for unlawful collection. As noted above, data users also need to be aware of telecommunications and surveillance legislation which prohibits or regulates the obtaining of particular types or information and/or by specified means.

Fairness of covert data collection - Some means of data collection might not be illegal, but they may still be a breach because they are unfair. This is particularly likely to be the case where the means of collection are covert (i.e. the subject is unaware of them). In our previous submission we cited relevant HK and NZ cases. While there have been no Australian privacy law cases to date on unfair *means* of collection, the Australian Privacy Commissioner has issued Guidelines on covert surveillance.

> ***Submission DP72-24: The Privacy Commissioner should be required to issue guidance about fair and lawful means of collection, which are of considerable practical importance.***

Cross reference to specific notification principle

The proposed UPP 2.4 seems redundant – it serves only as a cross-reference/reminder which has no place in a principle. It could be added as a 'note'.

> ***Submission DP72-25: UPP 2.4 should be deleted***

Other sources of information

We consider that the ALRC should have addressed in DP72 the issue we raised previously of whether the collection principle applies unambiguously to information obtained by observation or surveillance; to information extracted from other records, and to information generated internally as a result of transactions (CLPC IP 31, Submissions 4-4.2, 4.3 & 4.5)). These are important issues, and this review will be one of the few opportunities to influence how Courts will determine the future scope of the legislation. We repeat the substance of our arguments here, and re-iterate our previous submissions:

Observations / surveillance of the data subject

Personal information is obtained and recorded in many situations from observations of the data subject. We give examples in our previous submission. The observation may take place in the presence of and/or with the knowledge of the data subject, but may also be 'remote' and without their knowledge.[7] In many cases, observation will be by audio or video/CCTV. Given that most laws define personal information and/or records to include different storage media, it seems that the collection of personal information may also be in any medium, such as sound, photo or video, and not only text.

Most privacy laws are silent as to whether such observation constitutes 'collection', leaving the question to the ordinary meaning of collection. If the obtaining of these types of observed personal information did not constitute 'collection', then data protection laws would be drastically limited in scope and would ineffective in a wide range of practical situations. The requirements of minimum collection and fair collection methods should apply to collection by observation as much as to other forms of collection. The remedial nature of privacy laws suggests that observation should be included as collection. The practice of Privacy Commissioners seems to assume that such observation constitutes collection, and case law to the contrary is not known.

The more difficult question is whether the obligations to give notice on collection do apply in relation to collection by observation, or should apply. Whether observation is collecting 'from' a person seems uncertain. Whatever the position is under the current privacy principles, there is also uncertainty about under what circumstances notice should be required when information is collected by observation. One of the main functions of surveillance regulation laws is to specify under what circumstances notice of surveillance must be given, and under what circumstances covert surveillance is permitted. Should information privacy laws leave this question to separate surveillance laws? Some surveillance laws make a distinction between covert and overt surveillance, with lesser controls applying to 'overt' surveillance – defined as surveillance about which the individuals concerned have been made generally aware. Whatever position is taken on this question, the collection principle needs to clarify whether it requires notice to be given on collection by observation.

Information extracted

Much personal information is extracted from documentary or other sources. If information is not solicited from, or observed in relation to, any person, but extracted from a book or a database, is it 'collected'? The preferable view is that extraction is collection under current law, but the law would benefit from clarification on this point. From a policy perspective, it is desirable that collection includes extraction, so that the principles concerning minimum collection and fair collection will apply.

Information generated as a result of transactions with an individual

A possible further category of information held about individuals is information generated by the data user in the course of transactions – e.g. records of enquiries, service provision, purchases etc. In some instances this could be described as collection by observation, but in others that does not seem apt. Our view is that it is appropriate for all forms of collection of personal information to comply with the collection requirements that the collection be lawful, necessary, not unduly intrusive.

> ***Submission DP72-26: The law should make it clear that the collection principles UPPs 1 and 2 apply to the maximum practical extent to information obtained from observation or surveillance; to information extracted from other records, and to information generated within and organisation/agency as a result of transactions. This should be done either in the legislation or in the Explanatory Memorandum.***

As we have noted previously, it may be appropriate to modify the notification requirements where information is obtained by observation, surveillance or extraction, or generated as a result of transactions (CLPC IP 31, Submission 4-4.4). We note that specific notification is proposed to be a separate principle UPP 3.

> ***Submission DP72-27: Different notification requirements may appropriately be modified depending on how the data is collected, with the default position being that notice is required unless an exception is provided in UPP 3. The Privacy Commissioner should be required to issue guidance about compliance with the specific notification requirements under UPP 3 in relation to different circumstances of collection.***

5.7. Relationship between disclosure and collection

The ALRC has not addressed, in DP72, the issue we raised in our IP31 submission of how the purpose of collection is to be determined, so that it can be 'used' in the operation of the various principles that refer to purpose. In this context, our previous submission also canvassed the role of obligations of confidence, but this has also not been addressed (CLPC IP 31, Submissions 4-5.3 & 5.4). We repeat the substance of our arguments here, and reiterate our previous submission:

Relationship between disclosure and collection

How is the purpose of collection of personal information to be determined, so that it can be 'used' in the operation of the various principles that refer to purpose? In some circumstances, such as where collection requires and can accommodate notification, the purpose will need to be specified by the data user. However there are other circumstances, such as where information is obtained by observation or generated by transactions (see above) where there may not be an opportunity for notice. In such cases, the purpose of collection will have to be inferred from the circumstances and context, including any related prior notification (e.g. when individuals initially enter a relationship, such as becoming a welfare beneficiary, taxpayer, insurance policy holder or other customer).

An important example is where information is disclosed from one organisation to another. Where personal information is obtained from a third party which is also subject to privacy principles, what is the relationship between the purpose for which the information was held by the discloser, their intended purpose for disclosing, and the recipient's purpose of collection? Which purpose governs the recipient's subsequent obligations, including under the collection principles?

The obligations of those who receive personal information are complex, and derive from a number of sources.

Privacy principles do not simply say 'those who receive personal information are bound by the same obligations as the organisation from which they received it'. In fact, privacy principles rarely say anything direct about the obligations of the recipient of personal information (some exceptions are discussed below). Nor do privacy principles require a disclosing organisation to even state the purposes for which information is being disclosed, although they would, if challenged, need to be able to justify the disclosure under the relevant principle (see Use & Disclosure below).

Where a data user receives information legitimately disclosed under a privacy principle, and the recipient is aware of the basis of the disclosure, then that should condition and limit the purposes of their collection. It may be that purposes which would be lawful if the information was obtained elsewhere would not be acceptable under collection principles if they were not compatible with the disclosure authority of the source. But it is not clear if this would be based on the purpose being unlawful, or on the means of collection being unlawful or unfair. Where a data user knowingly receives information disclosed in breach of a disclosure principle (i.e. the source has no legal basis for the disclosure, and the recipient is aware of that fact) then it would seem clear that the collection is also in breach, in that the collector would be complicit in the unlawful disclosure (or in some cases may even have expressly solicited the unlawful act), and this would constitute unfair collection.

If the recipient data user is unaware of the basis of disclosure, then it cannot be expected to make this judgment, but the question arises 'is it under any obligation to enquire?' This would almost certainly depend on the circumstances. It might be reasonable, when collecting from established data users such as government agencies and large corporations, to rely on an assumption that they have a lawful basis for disclosure. In contrast, if there was any good reason to doubt that a disclosure is lawful (perhaps because it is inconsistent with previous experience, or where it was from a questionable source), then there might be an onus on the recipient to enquire or this would make the method of collection unfair. However, this is uncertain.

If a recipient's intended purpose(s) of collection are narrower than the purposes for which the source could disclose, the narrower purposes will be the relevant ones for privacy compliance purposes. Similarly, it the source only agrees to release information for a narrow purpose, even if they could themselves use the information for other purposes (e.g. where a finance company discloses data to a debt collector), it is the narrower purposes that will constrain the recipient.

The above propositions would make the law workable, but there is no authority for them. This is a key area where the meaning of privacy principles is uncertain.

> ***Submission DP72-28: The ALRC should address the issue of how Australian law should clarify the relationships between collection and disclosure of personal information, and in particular the limitations that the purposes of collection of a first organisation play in limiting the uses of a second organisation to which the information is disclosed. If this is not done in the legislation, it would nevertheless be valuable to have the Explanatory Memorandum clarify what is the expected interpretation of the legislation.***

<u>Obligations of confidence – role in limiting use and disclosure</u>

The law of breach of confidence can play a role in determining the purpose of collection and subsequent use and disclosure options (assuming circumstances of confidence apply and the information is confidential). The relationships to which confidentiality attaches is (surprisingly) still uncertain for many modern commercial and professional relationships beyond the well known relationships such as banker/customer and doctor/patient. The ALRC should ensure that its final report takes account of developments in relation to statutory powers and duties of confidence.

There is less uncertainty about the role of obligations of confidence is relation to government. Statutory obligations of confidence may also constrain uses and disclosures. The High Court's decision in *Johns v Australian Securities Commission* (1993) 178 CLR 408 that, in effect information obtained through the use of compulsory powers by a statutory body could not be used for purposes inconsistent with those powers has considerable but largely unexplored potential for interaction with privacy principles. The previous government once indicated an intention to seek legislative amendments to remove this constraint, which would have been a significant undermining of the purpose specification and limitation foundations of privacy law. We consider that, given the importance of this issue to the long-term development of privacy laws, the ALRC should, as far as is possible through the

Privacy Act, indicate the desirable relationship between breach of confidence laws and the protection of privacy. This is most feasible in relation to the federal public sector, which may also influence developments in relation to State and Territory public sectors.

> ***Submission DP72-29: The ALRC should address the issue of the role that the law of breach of confidence plays in determining the circumstances under which the use or disclosure of personal is limited. In particular the principles in Johns v ASC and similar cases, insofar as they apply to personal information, should be supported by statutory provisions in the Privacy Act.***

5.8. Notification requirements

The ALRC proposes that the notification requirements currently included in the private sector collection principle (NPP 1.3 & 1.5) should be dealt with in a separate principle (as it currently is for agencies (IPP 2)).

We support this proposal and provide comments separately on proposed UPP 3.

6. Specific Notification (UPP 3)

6.1. Introduction

ALRC proposed UPP 3

3.1 At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable steps to ensure that the individual is aware of the:

(a) fact and circumstances of collection (for example, how, when and from where the information was collected);

(b) identity and contact details of the agency or organisation;

(c) fact that the individual is able to gain access to the information;

(d) purposes for which the information is collected;

(e) main consequences of not providing the information;

(f) types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and

(g) avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information.

3.2 Where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of: (a) the matters listed in UPP 3.1 above; and (b) the source of the information, if requested by the individual.

3.3 An agency or organisation must comply with the obligations in UPPs 3.1 and 3.2:

(a) in circumstances where a reasonable person would expect to be notified; and

(b) except to the extent that:

(h) making the individual aware of these matters would pose a serious threat to the life or health of any individual;

(i) (ii) in the case of an agency, the agency is required or specifically authorised by or under law not to make the individual aware of one or more of these matters.

6.2. Location of notification requirements: separate principle?

We support the proposal to include notification under a specific separate UPP (DP72, Proposal 20-1). We suggested in our previous submission that a combined 'awareness' principle should be considered, combining the notification and openness principles, (CLPC IP31, Submission 4-1), and note that the OPC had a similar view. However, we think the ALRC has made a reasonable case in the DP72 for keeping these two principles separate.

6.3. Application of the notification principle

We support the ALRC's proposal that the UPP concerning notification should apply to both organisations and agencies (DP72, Proposals 20-1 & 20-2), for the reasons set out in paragraphs 20.18 to 20.20, and 20.45.

We support the ALRC's suggestion (explained in paragraph 20.30) that the notification requirements should generally apply to all circumstances of collection. In our view this should *expressly* include collection by observation, surveillance or internal generation in the course of transactions (see our comments below on UPP 3.1(a) and also on these different modes of collection in relation to UPP 2),

> ***Submission DP72-30: To ensure that all circumstance of collection are covered, the words 'by any means' should be inserted in UPP 3 as follows: '…..from the individual, by whatever means, it must take …'***

6.4. Objective of UPP 3

The aim of this principle is to ensure that individuals are aware of certain matters. If a data user can be satisfied that individuals about whom it is collecting personal information are aware of these matters there need be no specific notification. This might be because they have been made aware in some other way or by some other party (e.g. generic advertising campaigns), or where they have previously been informed by the same data user.

We are concerned that leaving the obligation as 'ensuring awareness' (as in NPP 1.3) is too open to abuse. For instance, as we have argued previously (in relation to our CLPC IP 31, Submission, 4-2), data users could deliberately omit privacy notices from routine communications even where there is minimal marginal cost in repeating it, relying instead on an initial communication constituting 'reasonable steps'. In our view, it is asking too much of individuals to expect them to remember the details of a privacy notice several months after they have received it, and in most contexts there is no good reason why notice should not be repeated.

We agree that the objective of this principle is to ensure awareness, but a better way of consistently achieving this objective would be, in our view, to slightly expand this principle from one that only refers to reasonable steps to 'ensure awareness' to one that requires reasonable steps to specifically 'notify' as the default action, with an option to otherwise ensure awareness, and a conditional exception where the data user could establish that at least the typical data subject had been made aware by other means (see our comment on UPP 3.1(a) below).

> ***Submission DP72-31: UPP 3.1 should be re-worded from '… reasonable steps to ensure that the individual is aware' to '…reasonable steps to notify the individual or otherwise ensure that the individual is aware' .***

6.5. When is notice not required?

We are concerned at the suggestion in paragraph 20.33 of DP72 that there will be a broad range of circumstances where no notification will be necessary. We believe that the case made here is far too simplistic. Just because an individual is aware that collection is taking place does not automatically mean that they are aware of all of the

matters to be included in normal notifications, and even if they have previously been notified, some of the details (such as intended recipients) may have changed over time.

Any exceptions should be narrow and specific. The exception embodied in UPP 3.3(a) is, in our view, far too subjective and also adopts the wrong 'default' setting. To the extent that an exception based on 'prior expectation' is justified, this should clearly *be* the exception; i.e. notification should be required *unless* there is a reasonable belief that most of the individuals concerned would not expect to be notified. Such a belief would most commonly be founded on a claim that individuals had already been made aware in some other way. There may also be some circumstances in which such a belief could be founded on evidence that individuals were not interested in knowing, although this could be more difficult to establish.

Submission DP72-32: UPP 3.3 should be re-worded as follows:

'An agency or organisation must comply with the obligations in UPPs 3.1 and 3.2 unless:

(a) it reasonably believes that the individuals concerned do not expect to be notified

The ALRC proposes an exception where making the individual aware would pose a serious threat to the life or health of any individual. (DP72, [20.25], and UPP 3.3(b)(i)). This carries over an existing exception to NPP 1.5, but would apply not only to collection from third parties but also to collection directly from the individual. There is no such current exception to NPP 1.3, and the ALRC has not provided any arguments to support this extension. Given that in the direct collection situation the individual will be aware that information is being collected, it seems unlikely that informing them of the matters covered by UPP 3.1 could cause any additional harm. In the absence of any justification, we oppose the application of exception (b)(i) to direct collection.

Submission DP72-33: UPP 3.3(b)(i) should only apply to indirect collection. As such, it may be better relocated to UPP 3.2.

The ALRC also proposes that UPP 3 should contain a further exception – that an agency not be required to comply with the relevant notification requirements if it is 'required or specifically authorised by or under law' not to make the individual aware, (DP72, [20.23] and proposed UPP3.3(b)(ii)).

Under the ALRC proposal, this exception would not be available to private sector organisations. We cannot see why it should not – there are such statutory constraints on businesses, such as the prohibition on 'tipping off' in the *AML-CTF Act* 2006 (s123).

We therefore support the proposed exception UPP 3.3(b)(ii) but submit that it should apply to agencies and organisations.

Submission DP72-34: Exception (b)(ii) in UPP 3.3 should apply both to agencies and to organisations.

6.6. Content of notice

***Fact and circumstances of collection*.**

We support the proposed inclusion in the requirement for an explanation of the fact and circumstances of collection (UPP 3.1((a)). However, we question whether the example – '(for example, how, when and from where the information was collected)' – belongs in the principle. It seems more appropriate for a 'Note' or further guidance to be issued later.

The express inclusion of the 'facts and circumstances of collection' is important because the knowledge that information collection is taking place does not automatically follow from the collection being 'from the individual'. In our comments on UPP2 we identified at least three categories of collection – by observation, by surveillance and from internal generation in the course of transactions to which the collection obligations should apply.

> ***Submission DP72-35: The explanation '(for example, how, when and from where the information was collected)' should be deleted from UPP 3.1(a) and given instead in a Note or further guidance.***

Collector's identity and contact details

We support the inclusion of these details, to apply to both agencies and organisations (UPP 3.1(b)). As we have previously suggested (CLPC IP 31, Submission 4-3) it may not be sufficient to rely on *any* contact details – they need to 'work' in terms of allowing genuine contact and a response. We suggest that consideration be given to adopting the terminology of the *Spam Act* 2003 which uses the term 'functional unsubscribe facility' to convey the requirement that the facility must work effectively.

> ***Submission DP72-36: UPP 3.1(b) should include the word 'functional' before 'contact details'.***

Access and correction

We support the inclusion of item (c) in UPP 3.1 but submit that it should also include a requirement to notify individuals of the important right to seek correction.

> ***Submission DP72-37: UPP 3.1(c) should read 'fact that the individual is able to gain access to the information and seek correction;'***

Purposes of collection and consequences of not providing

We support the inclusion of items (d) and (e) in UPP 3.1, which are carried over from NPP 1.3 (in the latter case, with some desirable simplification).

As we noted in our previous submission, the latter requirement is typically covered in a privacy notice – generally associated with indications as to which items of information are mandatory and voluntary information. The notice does not need to be too detailed but, at the least, should clearly indicate to individuals that if they don't give some (or all) of the information then they may not, for example, receive the services in question (CLPC IP 31, p. 25).

Submission DP72-38: We support the inclusion of items (d) and (e) in UPP 3.1

Usual disclosures

Submission DP72-39: We support the inclusion of information about usual disclosures as UPP 3.1(f).

The ALRC believes that privacy principles should not prescribe what level of detail is required in notification, but that OPC should provide guidance to assist agencies and organisation in ensuring that individuals are properly informed of the persons to whom their personal information is likely to be disclosed (DP72, [20.48] and Proposal 20-3). We accept that it is unrealistic to expect that it will always be practicable to list specific entities to which disclosures are made in privacy notices. However, where notices use *generic* descriptors of recipients (such as contractors, business partners, or government agencies), we believe there should be an additional obligation to answer specific enquiries about the specific identity of *actual* recipients. Without such a right, individuals will find it impossible to 'follow the trail' of their information, in the event of a problem. Such a right would complement the right that the ALRC accepts to request specific details of sources of information (see below).

We suggest that this right to request specific details of disclosures should be added as an additional obligation in UPP 4 (Openness), which already has an 'on request' element (in 4.2), and also because the same supplementary requirement should apply to some of the details in UPP 4.1 (see our submission below on UPP 4).

In the specific context of overseas transfers (see our comments on Chapter 28 and UPP 11), this obligation should require specification of the specific country or countries concerned – this can be achieved either by UPP 11 or by incorporation in our proposed new requirement in UPP 4.

Avenues of complaint

We support the ALRC's proposal that an individual should be made aware of avenues of complaint (DP72, [20.48] and Proposal 20-2).

Submission DP72-40: We support the inclusion of item (g) in UPP 3.1.

Notification where information collected from a third party

The ALRC accepts that it is generally appropriate, where an agency or organisation receives personal information about an individual from a third party, that it should retain an obligation to ensure that the individual is made aware of the matters prescribed in UPP 3.1 (DP72, [20.64], implemented through UPP 3.2(a)). We agree with this view.

The ALRC proposes in addition that where information is collected from a third party and the individual requests, an agency or organisation should be required to take reasonable steps to inform them of the source (DP72, [20.66] and Proposal 20-5). We suggest that this obligation needs to be made more explicit by referring to 'the identity of the source'. Otherwise, the source could be described simply in generic terms such

as credit bureau, or list broker, leaving the individual unable to pursue enquiries with any specific organisation.

> ***Submission DP72-41: Proposed UPP 3.2(b) should be amended to read: 'the identity of the source of the information, if requested by the individual.'***

We further suggest that the ALRC should expressly recommend that the drafting of UPP 3.2 makes it unambiguously clear that the 'if requested' qualification applies only to (b) and not also to (a), which must remain a pro-active obligation.

Timing of notice

The ALRC proposes that, where personal information is collected from individuals, the reasonable steps (to ensure awareness) should be taken at or before the time of collection or, if that is not practicable, as soon as practicable after (DP72, UPP 3.1). We support this but suggest that the OPC should be expressly required to issue guidance about the limited circumstances in which 'after the event' notification is acceptable.

Clearly, the objective of awareness – to put the individual in a position of knowledge before they decide whether to give up their personal information – is severely compromised if the information is not provided beforehand. On the other hand, there clearly are some circumstances where it is simply not practicable to convey all or, in some cases, any of the information in advance. The risk of providing a 'if impracticable then later' exception is that it can be abused, with data users who could provide the information prior to collection, perhaps with some cost or creativity, spuriously claiming 'impracticability'.

The ALRC proposes no timing condition where information is collected from a third party (UPP 3.2). This reflects an existing difference between NPP 1.3 and 1.5, which we consider to be unsatisfactory, for the reasons given above. We suggest that the 3.2 obligation be subject to the same timing qualification as 3.1. It is also necessary to clarify that the time referred to is the time of collection by the agency or organisation from the third party, not the original collection by the third party (although that will often be the way in which the obligation is fulfilled

> ***Submission DP72-42: Proposed UPP 3.2 should be amended at the end of the first paragraph to read '… the individual is or has been made aware, at or before the time of that collection (or, if that is not practicable, as soon as practicable thereafter) of:'***

Further guidance

We support the ALRC proposal that the OPC should provide guidance on various aspects of compliance with UPP 3 (DP72, Proposals 20-3, 20-6 and 20-7). However, as we have suggested above, far more of the detail of what the requirements mean in practice should be incorporated in the principle itself, leaving less to be covered in the guidance.

6.7. Technology Constraints on Notification

In our previous submission, we drew attention to the particular difficulties that may arise in communicating detailed privacy messages with certain modes of communication such as telephone calls, SMS and television advertising. (CLPC IP 31, p. 23) If communications by these modes invite direct response – for instance by the customer calling or texting – then, in theory, they should include information about the matters listed in the applicable notification principle.

This is impracticable in many increasingly common scenarios, and the common approach to compliance in relation to the various forms of direct response advertising is to rely on the 'if impracticable then later' exception – providing the relevant information either in later contact with the individuals concerned (e.g. when finalising a purchase, or sending a contract) or by reference to a website. Neither of these is satisfactory both because, as explained above, they deny individuals relevant information at the point of decision, and because there is even less chance than usual of the individuals locating and reading the relevant details.

Privacy laws face a major challenge in addressing 'non-traditional' means of communication. An extreme conclusion is that data users cannot comply and should not therefore use such channels to collect personal information, but this is unlikely to be acceptable either to consumers or business/government data users.

We consider that the ALRC has not addressed these issues in sufficient detail, given their importance to consumers now and in the future.

One approach to this problem is to accept that there will be an increasing incidence of personal information being collected without the preferred level of awareness, but strictly limiting the use that can be made of that information until such time as further information has been given. This approach is explored further in our comments on UPP 5 - Use and Disclosure.

7. Openness (UPP 4)

7.1. Introduction

ALRC proposed UPP 4

> *4.1 An agency or organisation must create a Privacy Policy that sets out the agency's or organisation's policies on the management of personal information, including how the personal information is collected, held, used and disclosed. This document should also include:*
>
> *(a) what sort of personal information the agency or organisation holds;*
>
> *(b) the purposes for which personal information is held;*
>
> *(c) the avenues of complaint available to individuals in the event that they have a privacy complaint;*
>
> *(d) the steps individuals may take to gain access to personal information about them held by the agency or organisation in question;*
>
> *(e) the types of individual about whom records are kept;*
>
> *(f) the period for which each type of record is kept; and*
>
> *(g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.*
>
> *4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual: (a) electronically, for example, on its website (if it possesses one); and in hard copy, on request.*

7.2. Separate 'Openness' Principle?

The ALRC proposes a discrete 'Openness' principle, separate from the 'Specific Notification' principle (UPP 3) to apply both to agencies and to organisations (DP72, [21.12] and Proposal 21-1).

> ***Submission DP72-43: We support Proposal 21-1 for a discrete Openness principle to apply both to agencies and to organisations.***

7.3. Matters to be included in a Privacy Policy

The ALRC proposes that the Privacy Policy sets out an agency's or organisation's policies on the management of personal information including the types of information, purposes for which information is held and avenues of complaint available, steps to gain access to information, types of individuals about whom records are kept, period for which each type of record is kept and the persons who can access the information and under what circumstances (DP72, Proposal 21-2 – UPP 4.1(a)-(g)).

> ***Submission DP72-44: We support Proposal 21-2 for the proposed content of UPP 4.1.***

7.4. Availability of a Privacy Policy

The ALRC proposes that agencies and organisations should be required to take reasonable steps to make their privacy policies available without charge both electronically, and, on request, in hard copy (DP72, Proposal 21-4 – UPP 4.2).

We support both these proposals. There is no excuse in the 21st Century for any entity not being able to make documents readily available through the Internet, but it is also important that those without electronic access can still obtain a hard copy if required.

> ***Submission DP72-45: We support Proposal 21-4 for the wording of UPP 4.2.***

The ALRC takes the view that agencies need no longer be required to submit a document to the OPC for the purposes of compiling a Personal Information Digest, as currently required by IPP 5.4(b) (DP72, [21.19]).

We disagree. We accept that there has been relatively little use of the Commonwealth (and ACT) Personal Information Digests over the 17 years they have been published. However, they remain a potentially valuable resource for the media and public interest groups to make comparisons and hold governments to account. Agencies will have to prepare the equivalent of a Digest entry in any case to satisfy UPP4, so the marginal cost is only that of annual submission and the compilation by the Privacy Commissioner. Now that these processes are established, the savings from removing the obligation would be very small, while a potentially extremely valuable resource would be lost.

> ***Submission DP72-46: UPP 4 should include a requirement: 'an agency must submit an electronic copy of its privacy policy to the Privacy Commissioner at least once each year'.***

To maximise the value of these submitted privacy policies, OPC should be required to provide them online, so that they available in a consolidated collection. While OPC may be able to add some value to this information (e.g. provision of a search engine), other parties may be able to add different and complementary values by processing the Privacy Policies in different ways (e.g. different search engines, adding hypertext links to other resources). Provided republication of such policies is accurate it should be allowed as a means of increasing openness of privacy policies.

> ***Submission DP72-47: Any privacy policies submitted to the Privacy Commissioner should be published by the Privacy Commissioner, and may be republished by other parties'.***

While it would be unnecessary, bureaucratic and costly to require all private sector *organisations* to similarly submit their privacy policies, the Commissioner should be able to require classes of organisations to submit their policies for similar re-publication, where the public interest in such convenient access justifies this because of the privacy sensitivity of the particular organisations and the information they hold. Such requirements should be by legislative instrument so as to provide the check of disallowance.

Submission DP72-48: The Privacy Commissioner, by legislative instrument, should be able to require a class of organisations to submit an electronic copy of their privacy policies to the Privacy Commissioner at least once each year.

We also support a requirement for both agencies and organisations to provide further details of their information management to the Privacy Commissioner on request. This is best located elsewhere in the Act and we take it up in our submission on Part F of DP72.

7.5. Guidance

The ALRC proposes that the OPC should issue guidance on how agencies and organisations can comply with their obligations under the proposed 'Openness' principle to produce and make available a Privacy Policy (DP72, Proposal 21-3).

We support Proposal 21-3.

7.6. Short Form Privacy Notices

The ALRC takes the view that best practice by agencies and organisations is to create 'layered' privacy notices (a comprehensive version and an abbreviated summary) (DP72, [21.46]). However, it suggests that it is more appropriate for the OPC to encourage and guide the adoption of this practice, rather than mandating it in the *Privacy Act* (DP72, [21.47] and Proposal 21-5).

As we noted in our earlier submission, many consumer representative organisations, while acknowledging an 'information overload' problem, view trends towards layered and short form privacy notices with suspicion, as they can too easily omit information which should be relevant to an individual's decision whether to proceed with a transaction.

We believe that it is necessary to mandate a minimum level of information to be provided at or before the time of collection and a minimum standard of transparency and ease of navigation between specific collection notices and privacy policies. This is best achieved either in Regulations or a binding Code.

Submission DP72-49: Regulations or a binding Code should prescribe the minimum set of information which needs to be provided at or before the time of collection to achieve the objective of the specific notification principle (UPP 3) and the minimum standard of transparency of links to more detailed information provided under UPP 4.

8. Use and Disclosure (UPP 5)

8.1. Introduction

ALRC proposed UPP 5

5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose***) other than the primary purpose of collection unless:*

(a) both of the following apply:

(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to:

(i) an individual's life, health or safety; or

(ii) public health or public safety; or

(d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or

(e) the use or disclosure is required or authorised by or under law; or

(f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

5.2 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

Note: *Agencies and organisations are also subject to the requirements of the 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.*

8.2. A single 'Use and Disclosure' principle?

The ALRC proposes that the UPP should contain a single use and disclosure principle that applies to agencies and organisations (DP72, [22.22] and Proposal 22-1).

There are competing arguments. A single principle avoids arguments about whether an action is a use or a disclosure and therefore which principle applies. On the other hand, separate principles allow each to deal with issues that arise specifically in the context of internal use or of disclosure to third parties. But the concept of a third party is slippery, particularly with large multi-function data users. Corporate entities can have many different 'business lines' and government agency boundaries are constantly changing with new administrative arrangements and portfolios. The NSW ADT has ruled that under PPIPA, in relation to agencies with disparate functions, some internal uses can be disclosures[5]. Even with a single principle, it is still necessary to understand the meaning of the two concepts.

> ***Submission DP72-50: On balance, we support Proposal 22-1 for a single 'use and disclosure' principle.***

8.3. Meaning of terms

In our previous submission, we urged the ALRC to consider the importance of the meaning of the terms 'use', 'disclosure' and 'purpose of collection' in the context of this principle. There is little discussion of this in DP 72, apart from a brief conclusion in paragraph 22.24, on which we comment below, and we consider that this is inadequate given the importance of these terms to the meaning of the Act. We therefore repeat here the substance of our previous arguments, and largely re-iterate our previous submissions, with some modifications as to how the objectives can be achieved.

Meaning of 'use'

The UK case of *R v Brown* [1996] 1 AC 543, a case on UK privacy legislation, held that merely reading personal information is not 'use' of that information. In contrast, the Federal Privacy Commissioner's *Plain English Guidelines to Information Privacy Principles 8-11* (1996) states that 'As a general rule, any accessing by an agency of personal information in its control is a "use"', and this includes 'searching records for any reason'.

> ***Submission DP72-51: Either this principle, the definitions, or the Explanatory Memorandum, should confirm that accessing personal information, even without further action being taken as a result of that access, is 'use' of personal information.***

As noted in paragraph 4.33 of IP 31, the *Privacy Act 1988* s.6 provides that '***use***, in relation to information, does not include mere disclosure of the information, but does include the inclusion of the information in a publication.' The meaning of this has always been unclear. In relation to Commonwealth agencies, the Federal Privacy Commissioner has considered many situations where an agency passes personal

[5] *KJ v Wentworth Area Health Service* [2004] NSWADT 84.

information to an outside organisation or agency to be a 'use' not a 'disclosure', applying a test of 'whether or not the agency maintains control over that personal information'. It seems that outsourcing of processing of personal information has been dealt with in this way (see Federal Privacy Commissioner, 'When is passing personal information outside an agency a use?' in *Plain English Guidelines to Information Privacy Principles 8-11* (1996)). It is questionable whether this interpretation would be upheld by a Court if challenged, and it would be unwise to simply apply it in the private sector context without further consideration.

> ***Submission DP72-52: Either this principle, the definitions, or the Explanatory Memorandum, should clarify the circumstances in which passing information outside an organisation remains a use rather than a disclosure***

Meaning of 'disclosure'

The ALRC confirms (in DP72, [22.24]) that disclosure can include 'revealing' or 'making accessible'. This implies that there can be a disclosure even if the information is not used or acted on by the third party (although there would presumably be an objective test of whether anyone had actually viewed the information). We suggest that this needs to be made clear either in this principle or in definitions.

We argued in our earlier submission that 'disclosure' should include information already known to the recipient,[6] and that this is of considerable practical importance (CLPC IP31, p. 28).

> ***Submission DP72-53: Either this principle, the definitions, or the Explanatory Memorandum, should make it clear that there can be a disclosure even if the information is not used or acted on by the third party, and that even information already known to the recipient it can still be 'disclosed'.***

Meaning of 'purpose of collection'

We asked in our earlier submission if there can be more than one distinct original purpose of collection? While NPP 1.3(c) refers to notice of 'the purposes for which the information is collected', the Commissioner has taken the view that there will only ever be one primary purpose, with all other purposes being secondary (Guidelines to the NPPs - NPP 2.1(a)) The problem with this view is that it invites data users to define their purpose broadly so as to avoid the constraints on secondary purposes. The EU Directive, by contrast, stipulates that the purposes for which data are collected shall be 'specified' and 'explicit' (Article 6(1)(b)). This is generally taken to mean that the purposes must be delineated in a relatively concrete, precise way (see further Bygrave, 2002, p.338).

We have assumed in our comments on the Collection principle (UPP 2) that there may be multiple purposes.

---

[6] Patrick Gunning, *Disclosure of personal information* in Gunning, 2001 and Graham Greenleaf, *Does disclosure include information already known?* in Greenleaf, 2001.

Another issue we identified that has not been adequately addressed by the ALRC is how broad an original purpose should be permissible. We have dealt with some aspects of this issue, including the issue of 'bundling' in our submission on Chapter 16 – Consent.

Submission DP72-54: The law should be clarified to expressly allow for the declaration of multiple specific purposes, but not to allow a broadly stated purpose .

8.4. Exceptions to the limitation on use and disclosure

UPP 5, like NPP 2, starts from the premise that personal information should only be used or disclosed for the primary purpose for which it was collected, unless …. Various exceptions are then proposed, based on those in NPP 2, but with some suggested variations.

Exception for a related secondary purpose

The ALRC believes that a *direct* relationship between the secondary purpose and the primary purpose is not required in the in the 'related purpose' exception in the use and disclosure principle so far as it relates to non-sensitive information (DP72, [22.38]-[22.42] and Proposal 22-2). A direct relationship should continue to be required in relation to sensitive information (DP72, [22.43] and Proposal 22-2). This continues the distinction made in NPP 2. We have argued previously for the direct relationship test to apply to both sensitive and non-sensitive information, but now accept that this is not justifiable in relation to non-sensitive information given the second test proposed.

The ALRC proposes a continuation of a second test in this exception – that the use of disclosure be within the reasonable expectation of the individual. (DP72, [22.42] and Proposal 22-2). We support the inclusion of this 'reasonable expectation' test.

Submission DP72-55: We support the proposed exception UPP 5.1 (a).

Exception for consent (UPP 5.1(b))

We support the inclusion of this exception, subject to our general comments about consent – see our response to Chapter 16.

Submission DP72-56: We support the proposed exception UPP 5.1 (b).

Exception for emergencies and threats to life or health (UPP 5.1(c))

The ALRC concludes that the current exceptions regarding 'emergency' situations are too narrow. The ALRC proposes to delete 'imminent' from the requirement that a threat must be both serious and imminent to satisfy this exception (DP72, [22.64] and Proposal 22-3).

The ALRC proposes to retain the threat categories in NPP 2.1(e)(i), that is, where an individual's life, health or safety or public health or public safety is threatened (DP72, [22.65] and Proposal 22-3])

The arguments put forward to support the removal of the word 'imminent' in this exception have in our view been largely addressed by the 'emergencies and disasters' amendments to the *Privacy Act* in late 2006 [7]. We suggest that it is only if it becomes evident over time that these amendments have not adequately addressed the concerns that further amendments, such as a major broadening of this exception, be considered.

We re-iterate our belief that most of the examples of what has become known as 'BOTPA' (Because of the *Privacy Act*…) involve a misinterpretation of the constraints – sometimes out of ignorance but too often from laziness; unwillingness to explore the statutory exceptions and discretions or a wilful desire to blame the law for something that the data user does to wish to do for some other reason.

Removal of the 'imminent' element from the harm test would probably be acceptable in relation to the first part of the exception - threat to '(i) ***an individual***'s' life, health or safety. It would however be very dangerous in relation to the second part – threat to '(ii) public health or public safety.'

This is because there is currently no constraint on the ability of an agency or organisation to claim this exception for bulk or routinised uses or disclosures, as opposed to ad hoc, specific individual circumstances. The first part of the exception is by definition so limited – it will be necessary to identify specific individuals or small groups to satisfy this test. But if the exception was available for public health and public safety without the 'imminent' test, it is difficult to see how claims could not be made under it for a wide range of law enforcement and welfare programmes, including high volume data-matching and data linkage projects.

We submit that it was clearly never the intention of Parliament for this exception to provide an alternative basis for such programmes. They should instead have to satisfy one of the other exceptions – typically 'by or under law' – see below.

The only condition on which the deletion of 'imminent' might be acceptable would be if the exception was limited to ad-hoc case by case circumstances. In the absence of any such limits, we oppose the proposed change.

Submission DP72-57: We oppose the deletion of the qualifying word 'imminent' from UPP 5.1(c)

Missing persons

The ALRC's view is that issues relating to missing persons are assisted by other proposals, and does not believe it is desirable to create a further specific exception in relation to missing persons (DP72, [22.78]). We support this view.

Exception relating to suspicion of unlawful activity (UPP 5.1(d))

The ALRC believes that this exception, based on the current NPP 2.1 (h) should also apply to agencies (DP72, [22.77]).

Submission DP72-58: We support the proposed exception UPP 5.1 (d).

---

[7] *Privacy Legislation Amendment (Emergencies and Disasters) Act 2006* (Cth).

Exception where by or under law (UPP 5.1(e))

The ALRC canvasses views on the narrowing of the exception currently found in NPP 2.1(g) to include only where a use or disclosure for a secondary purpose is either required or 'specifically' authorised by or under law. (DP72, Question 22-1)

We agree with the reasoning of the ALRC that lead to this proposal, and support the narrower wording. No compelling examples have been provided in support of the status quo.

> ***Submission DP72-59: We support a narrowing of the proposed exception UPP 5.1 (e) to include 'specifically'.***

Exception for assistance of enforcement bodies (UPP 5.1(f))

This exception is carried over from the existing NPP 2.1(h). We refer to our comments on the similar exceptions in UPPs 9 and 11 that this exception implies the *active* involvement of an Australian enforcement body (as defined in the Act). It should not be open for an agency or organisation to claim this exception in respect of uses or disclosures which were only of *prospective* interest to an enforcement body. The correct and preferable exception for those circumstances is the reasonable suspicion of unlawful activity – UPP 5.1(d).

> ***Submission DP72-60: We support the proposed exception UPP 5.1 (f). We suggest that there should be a Note to this exception stating that it requires the active involvement of an Australian enforcement body***

8.5. Other exceptions?

The ALRC's view is that it is unnecessary to include an additional exception in the use and disclosure principle to allow for disclosure of incidents to insurers (DP72, [22.91]). We support this view.

The ALRC believes that there is no need to create a new exception dealing with the use and disclosure of personal information in the course of due diligence (DP72, [22.99]). We support this view.

The ALRC deals with issues of research and health care in Part H of DP72, with a view to moving these provisions out of the 'Use and Disclosure' principle in the proposed UPPs and into more specific subordinate legislation" (DP72, [22.101]). We comment on these proposals and issues in our submission on Part H.

We note that in Chapter 40, dealing with other exemptions, the ALRC asks if exemptions or exceptions are needed for alternative dispute resolution (ADR) bodies (DP72, Question 40-2). We comment on that suggestion in our separate submission on Part E of DP72.

8.6. Logging uses and disclosures for secondary purposes

The ALRC does not believe that it is desirable to require agencies and organisations to record their use or disclosure of personal information when this occurs for a purpose other than the primary purpose of collection (DP72, [22.114]). We are very disappointed with this conclusion and urge the ALRC to reconsider. If designed into

systems, recording of exceptional uses and disclosures should be both easy and cheap, and would in our view have a wide range of collateral benefits. Good record-keeping is simply good business practice.

The ALRC suggests that the record keeping requirement be retained as it relates to use or disclosure under the relevant law enforcement exception (DP72, [22.117]). However there is no firm proposal to this effect and it is missing from the proposed UPP 5.

> ***Submission DP72-61: UPP 5 should include a specific requirement to keep a log or record of all uses and disclosures for secondary purposes under exceptions (a)-(f).***

8.7. Significance of exceptions

As we stated in our earlier submission, the exceptions are not in themselves *requirements* to disclose (or use) personal information. Organisations may choose not to disclose information even if it is not a breach of a principle to do so, unless some other law compels them to disclose. Nor are exceptions *general authorisations* to disclose: a disclosure compliant with an exception may still leave the discloser open to other actions for wrongful disclosure, whether because of some breach of another statute, or a breach of confidence, or a breach of copyright, or some other action. If the discloser has an obligation not to disclose which arises outside privacy laws, an exception to a disclosure principle cannot act as a defence. The same applies to uses which breach other duties.

It is very easy for data users or data subjects to overlook or not understand this limited role of exceptions to privacy principles, and it may be valuable to remind them of this. The best place to do so is in the Act itself, by a note. Alternatively, but less usefully, the Explanatory Memorandum could be used. Those who wish to encourage data users to disclose information in circumstances where an exception applies may not point out this limited role, resulting in data users mistakenly believing they have an obligation to disclose, or that they need no consider other legal obligations before they do so.

The NSW PPIPA contains a specific provision making clear that exceptions do not constitute obligations to disclose (s.23(6)).

> ***Submission DP72-62: There should be a clear statement, either by note in the Act (the preferred option) or in the Explanatory Memorandum in relation to UPP 5 that all the exceptions apart from (e) are discretionary and are neither a requirement nor an authorisation to use or disclose.***

9. Direct Marketing (UPP 6)

9.1. Introduction

The ALRC proposes a special direct marketing privacy principle which would apply regardless of the purpose for which the information was collected, requiring that direct marketing only occur where an individual has given consent, unless it is impracticable to gain consent. It would allow individuals to opt out at no charge under any circumstances, and require express consent for marketing use of sensitive information. This would make the current private sector provisions more comprehensive, but the ALRC is still undecided about whether it should apply to the public sector.

ALRC proposed UPP 6

6.1 An organisation must not use or disclose personal information about an individual for the primary purpose or a secondary purpose of direct marketing unless all of the following conditions are met:

(a) the individual has consented, or both of the following apply:

(i) the information is not sensitive information; and

(ii) it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and

(b) the organisation will not charge the individual for giving effect to a request by the individual to the organisation not to receive direct marketing communications; and

(c) the individual has not made a request to the organisation not to receive direct marketing communications, and the individual has not withdrawn any consent he or she may have provided to the organisation to receive direct marketing communications;

(d) in each direct marketing communication with the individual, the organisation draws to the individual's attention, or prominently displays a notice, that he or she may express a wish not to receive any further direct marketing communications; and

(e) each written direct marketing communication by the organisation with the individual (up to and including the communication that involves the use) sets out the organisation's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the organisation can be contacted directly electronically.

6.2 In the event that an individual makes a request of the organisation not to receive any further direct marketing communications, the organisation must comply with this requirement within a reasonable period of time.

6.3 An organisation must take reasonable steps, when requested by an individual to whom it has sent direct marketing communications, to advise the individual from where it acquired the individual's personal information.

9.2. Definition of 'direct marketing'

We suggest that it will be necessary to define 'direct marketing' for the purposes of this principle. To ensure that the objective of the proposed Direct Marketing principle is met, it is essential that it is defined broadly to include direct approaches to individuals about any matter, including but not limited to offers of goods or services, fundraising, and promotion of political, religious or charitable aims, including offers of membership.

Too much of the media-specific regulation introduced recently (such as the *Spam Act* 2003 and *Do Not Call Register Act* 2006) has been undermined by broad exemptions for activities which individuals typically regard as at least as intrusive as marketing of goods or services.

It is also essential to dispel any implied limitation of the definition to marketing where the fulfilment is by direct means (e.g. mail order). The direct marketing industry has in the past sought to limit regulation to direct sales, leaving out marketing the intention of which is to entice consumers into a retail outlet.

> ***Submission DP72-63: The Privacy Act should define 'direct marketing' as 'the marketing or promotion of goods, services or ideas, including fundraising and recruitment, by direct targeted communication with specific individuals or by individualised communications, by any means.'***

The words 'or by individualised communications' refer back to our proposed clarification of the meaning of 'personal information'. So, for example, customised marketing based on the use of 'cookies' would be covered irrespective of questions of whether other information allowed the marketer to know the identity of the marketing prospect.

See also our comments on the media-specific direct marketing laws in our submission on Part J of DP 72.

9.3. A separate principle

The ALRC proposes a separate principle to regulate direct marketing, whether it is the primary purpose for which personal information was collected or a secondary purpose (DP72, [23.21-22] and Proposal 23-1).

> ***Submission DP72-64: We support Proposal 23-1 for a separate Direct Marketing principle.***

9.4. Application of the Principle

Agencies?

The ALRC asks if this UPP should apply to agencies as well as to organisations (i.e. the private sector) (DP72, Question 23-1). We believe it should so apply on the grounds that the boundaries between private and public sectors are increasingly blurred, and government agencies are now commonly undertaking direct marketing

activities. As we noted in our earlier submission, the equivalent principle in the Hong Kong Ordinance applies to all sectors, and the Hong Kong Privacy Commissioner has found public sector bodies in breach of it. Government agencies will still be able to justify some direct marketing campaigns – the proposed principle accommodates this, while giving individuals the choice not to receive some government communications through these channels. Governments can generally rely on generic 'broadcast' media to promote services, compliance issues etc.

> ***Submission DP72-65: UPP 6 should apply both to agencies and to organisations.***

Sensitive information

The effect of the ALRC's proposal, as implemented in UPP 6.1(a), is that any use of *sensitive* personal information for direct marketing will require consent – i.e. the allowance for consent being impracticable in 6.1(a)(ii) does not apply to sensitive information.

We support the construction of the principle to have this effect, subject to our generic comments on consent in our submission on Chapter 16 of DP 72.

9.5. Exceptions

By or under law

If, as we suggest, the principle applies to agencies, then there will need to be an exception to allow direct marketing where it is required or specifically authorised by or under law. While it is difficult to see legal 'requirement' for direct marketing arising, it should be left in to cover the possibility. Given the increasing delivery of government services through the private sector, such an exception should also apply to organisations.

> ***Submission DP72-66: UPP 6 should contain another exception as an alternative to conditions (b)-(e) so that 6.1 would read: '… unless the following conditions are met:***
>
> ***(a) [as proposed by the ALRC]***
>
> ***and either***
>
> ***(b) the use of information for direct marketing is required or specifically authorised by or under law,***
>
> ***or***
>
> ***(c) all of the following conditions are met:***
>
> ***[(b)- (e) in current proposal renumbered as sub-items within (c)]***

Consent

The ALRC proposes that the Direct Marketing principle allows use of personal information for direct marketing where the individual has consented (UPP 6.1(a)).

We support this exception but subject to the comments we make generically about consent in our submission on Chapter 16 of DP 72.

9.6. Relationship to other laws

The ALRC proposes that the general requirements of proposed UPP 6 should continue to be displaced by more specific sectoral legislation (DP72, Proposal 23-2).

This should go without saying – it must always remain possible for specific legislation to override generic laws. At present, both the *Spam Act 2003* and the *Do Not Call Register Act 2006* have this effect, generally strengthening the limits in the generic NPP 2.1(c). However, we suggest that the ALRC should not remain neutral, but should instead recommend that any sectoral legislation addressing direct marketing should as far as possible be consistent with UPP 6, and that any weakening of the standards in UPP 6 should be clearly justified.

> ***Submission DP72-67: Any sectoral legislation addressing direct marketing should as far as possible be consistent with UPP 6. Any weakening of the standards in UPP 6 should be clearly justified and should be included in the Privacy Act as exceptions to UPP 6.***

9.7. 'Opt out' default

The ALRC proposes that UPP 6 should require individuals to be presented with a simple means to 'opt-out' of receiving direct marketing communications (DP72, Proposal 23-3).

We support this proposal, but suggest that it is strengthened in a number of ways. (We also suggest that the ALRC reviews the construction of 6.1 with a view to avoiding the double negatives in conditions (b) & (c), which make it quite difficult to understand).

Firstly, we see no reason to limit the communications in which contact details are provided. The qualification '(up to and including the communication that involves the use)' should be removed from proposed UPP 6.1(e).

Secondly, there should be a specific requirement that the means presented be 'functional' – i.e. able to achieve the intended effect. This is based on the 'functional unsubscribe facility' requirement in the *Spam Act 2003*. Without such a qualification, there would be myriad ways in which organisations (or agencies) could frustrate the objective of the 'opt-out requirement by making it difficult or impossible for individuals to exercise the choice.

Thirdly, there is no need for the principle to use such technology- or media- specific language. The principle only needs to convey the objective that whatever medium is used, the means of reply must be at least as easy to use.

> ***Submission DP72-68: UPP 6.1(e) should be amended to read '….each communication by the [organisation] with the individual includes a functional means of contacting the [organisation]. If the communication is by electronic means, the means of contact must be at least as easy to use.***

Lastly, individuals should be able to indicate their preference not to receive direct marketing communications either by direct contact with an organisation [or agency] or through any general preference scheme to which the organisation [or agency] is subject. This would ensure that organisations [and agencies] had to respect individuals' preferences registered with such schemes as the statutory Do Not Call Register or the voluntary ADMA Do not Mail service, to the extent that they were bound (either by law or by subscription) to use such schemes.

Submission DP72-69: UPP 6.1(c) should be amended to read 'the individual has not made a request, either directly or indirectly, to the [agency or] organisation …'.

9.8. Response times

The ALRC proposes that UPP 6 should require [organisations] involved in direct marketing to comply, within a reasonable time, with an individual's request not to receive direct marketing communications (DP72, Proposal 23-4).

We support this proposal, but urge that it be strengthened by the prescription, in Regulations or a binding Code, of specific target response times for different media of communication.

Submission DP72-70: Either Regulations or a binding Code should prescribe specific response times for different media of communication, to give effect to individuals' requests not to receive further direct marketing communications.

9.9. Information about sources

The ALRC proposes that individuals should have a right to request information about where an organisation that has sent a direct marketing communication has acquired the individual's personal information (DP72, Proposal 23-5).

We support this proposal, but urge that it be made more specific by requiring information on the identity of the source. Without this qualification, the principle could be satisfied by a broad generic description (e.g. list brokers) which would be of limited value to an individual seeking to 'follow the chain' of information, which the ALRC notes is one of the objectives (DP72, [23.62]).

Submission DP72-71: UPP 6.3 should be amended to read '…to advise the individual of the identity of the source of the individual's personal information.'

9.10. Further guidance

The ALRC proposes that the Office of the Privacy Commissioner should issue guidance on two specific matters relating to direct marketing – data quality and vulnerable people (DP72, Proposal 23-6). We support this proposal, but suggest that there will also be a need for advice on how to implement the requirements of UPP 6 in relation to specific communications media – in particular the difficulties of communicating much detail when using voice telephony and SMS/MMS or instant messaging.

Submission DP72-72: The Privacy Commissioner should be required to issue guidance about compliance with UPP 6, including specifically the matters specified in proposal 23-6, and the practicalities of compliance when using different communications media.

10. Data Quality (UPP 7)

10.1. Introduction

The ALRC proposes two extensions of the data quality principle to require collectors to take reasonable steps to ensure that personal information they collect, use or disclose is relevant. Presently, NPP 3 is limited to accuracy, timeliness and completeness, while the IPPs do not impose data quality requirements at the time of disclosure.

ALRC proposed UPP 7 - Data Quality

> *An agency or organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the UPPs, accurate, complete, up-to-date and relevant.*

10.2. Extension to scope of the principle supported

We support the ALRC's move to a single privacy principle dealing with data quality applicable to both agencies and organisations (DP72, [24.9] and Proposal 24-1)

We support the ALRC's view that it is unnecessary to include a provision in the proposed data quality principle explicitly stating that the obligations in the principle are not absolute, as the reference to 'reasonable steps' is sufficient (DP72, [24.33]).

A statement needs to be included either in a Note in the Act or in the relevant Explanatory Memorandum that in assessing what is reasonable, primary regard shall be given to the extent to which data-processing error can have detrimental consequences for the data subject(s) (see Bygrave 2002, p.368). This would help offset attempts by data controllers to place primary weight on their own needs when assessing what is reasonable.

> ***Submission DP72-73: There should be a clear statement, either by note in the Act (the preferred option) or in the Explanatory Memorandum that in assessing what steps are reasonable under UPP 7, primary regard shall be given to the extent to which data-processing error can have detrimental consequences in the context of the particular information and circumstances.***

We support the uniform extension of the data quality principle to apply at the time of disclosure (DP72, [24.4]).

The ALRC believes that the data quality principle should only be extended to data collectors that collect, use or disclose personal information (DP72, [24.20]). The question of whether this principle should apply to information a data user 'controls' is applicable to all principles and is discussed in the part of our submission responding to Chapter 3.

The ALRC believes that the principle should require in all circumstances that the information should be relevant to the purpose for which it was collected or a permitted secondary purpose (DP72, [24.22]). We support this stance. The change will also assist Australia's law to meet the standards of the EU Directive, although (as set out in CLPC IP 31, p. 43), this was not likely to be a significant issue in relation to

the Data Quality principle.

10.3. Quality obligations should apply to secondary and improper uses

The ALRC proposal measures the quality standards relative to 'a purpose of collection', but if personal information is to be used for a secondary purpose (use or disclosure) permitted by the UPPs then the agency or organisation should be required to ensure that it is of appropriate quality for that use or disclosure, which may be quite different from the purpose of collection.

This is consistent with the OECD requirement that information be 'relevant to the purposes for which they are to be used.' The ALRC recognises this, and refers to quality being understood with reference to the purpose of collection 'or another purpose permitted under the privacy principles' (DP72, [24.22]), so it seems this qualification may have been omitted in error.

This argument applies whether or not the secondary use is a use permitted under the UPPs, because if use is made of irrelevant or out-of-date information for purposes which are also improper, this use is still a breach of the quality principle.

However, the one exception is where an agency or organisation is required by law to disclose information. In such a case, the agency or organisation does not then have any control over whether to disclose, and cannot reasonably be expected to consider data quality relative to the requester's purpose (although it should draw any obvious quality limitations to the attention of the requesting party). However, if an agency or organisation makes its own decision to disclose, it should also have the responsibility to decide whether the information it discloses is of the required quality.

> ***Submission DP72-74: UPP 8.2 should state 'An agency or organisation must take reasonable steps to ensure that the personal information it uses or discloses for a purpose other than the purpose of collection is accurate, complete, up-to-date and relevant in relation to that purpose, unless it is required by law to disclose the information.'***

10.4. Automated Decision-making

In 15.6 below, we suggest a sub-principle, to be added to UPP 8, concerning automated decision-making.

11. Data Security (UPP 8)

11.1. Introduction

The ALRC proposes that the UPPs should contain a principle called 'Data Security' that applies to agencies and organisations (DP72, Proposal 25-1). We support this proposal. The ALRC's UPP 8 combines three somewhat distinct principles which are nevertheless related by considerations of risks of misuse of personal information: (a) security; (b) restrictions on retention (or obligations to destroy / de-identify); and (c) obligations to ensure proper use by third parties. We deal with each separately.

ALRC proposed UPP 8 - Data Security

> *An agency or organisation must take reasonable steps to:*
>
> *(a) protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure;*
>
> *(b) destroy or render non-identifiable personal information if it is no longer needed for any purpose permitted by the UPPs; and*
>
> *(c) ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the UPPs.*

11.2. Data security proposals

Elements of 'security'

The ALRC's formulation in (a) of the risks against which security must protect is not broad enough. 'Misuse and loss' by authorised users will not necessarily encompass excessive accesses or accidental alteration or degradation falling short of loss. The reference to 'unauthorised access, modification or disclosure' implies that 'loss' and 'modification' have different meanings, and it may be that neither includes the other. If so, then security need not protect against loss of data caused by unauthorised parties – which would be ridiculous. The expression 'or other misuse' as used in the draft Asia-Pacific Privacy Charter can usefully be used to ensure comprehensiveness in relation to both authorised and unauthorised users.

> ***Submission DP72-75: UPP8 should be re-worded to require protection against 'improper access, use, alteration, deletion or disclosure, or other misuse, by both authorised users and by other parties'.***

Reasonable steps test

We support the ALRC's uses of 'reasonable steps' as the principal test for what is required in all three elements of this principle, rather than trying to enumerate elements of security in the legislation.

However, there is a significant risk of misuse of security concerns by the over-zealous application of UPP 8(a) or (c), resulting in privacy protections which themselves become privacy infringements, and serve to impede the legitimate flow of personal information. As noted in our previous submission, the draft Asia-Pacific Privacy

Charter tries to guard against this by referring to 'security safeguards commensurate with [the information's] sensitivity, and adequate to ensure compliance', and the APEC Privacy Framework is even more explicit in requiring that:

> Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.

We consider that the ALRC should adopt some such formulation as a caveat on all of UPP 8(a)-(c) (see CLPC IP31, Submission 4-17).

Submission DP72-76: UPP 8 should also state that 'For the purposes of this Principle, reasonable steps must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information.'

The ALRC proposes that the OPC should provide guidance about the meaning of 'reasonable steps' in the context of the proposed 'Data Security' principle, and specifies the matters to be dealt with in this guidance (DP72, Proposal 25-3).

We submit that it is more useful for all concerned if OPC is *required by the Act* to issue such guidelines, rather than this merely being a suggestion buried in an ALRC report. Statutory requirements will be complied with by OPC, whereas mere ALRC recommendations, even if accepted and 'endorsed' by the government, may not be. They can also be used by OPC to mount a case for additional resources which may be needed to ensure compliance. Otherwise, lack of resources may be used as an excuse for delay in implementing what is only an ALRC suggestion. There is nothing unusual about Privacy Commissioners being required to issued guidelines or codes within a specified period after legislation comes into force. It happened in Australia in relation to tax file numbers and credit reporting, and it happened in Hong Kong in relation to ID numbers.

Submission DP72-77: OPC should be required by the Act to issue guidelines on the meaning of 'reasonable steps' within one year.

We refer to our general reservations about OPC Guidelines in our submission on the Commissioner's role (Response to DP72 Part F).

11.3. Non-retention (destruction or non-identifiability)

Extension of non-retention requirements to agencies

The ALRC proposes that personal information held by an agency or organisation should be destroyed or permanently de-identified ('rendered non-identifiable) when no longer needed. This rule should be able to be displaced by specific legislation. (DP72, [25.40]).

We support ALRC Proposal 25-4 concerning UPP 8(b) which, for the first time, would subject government agencies to a non-retention principle, although we adhere to the view that this should be in a separate principle (see CLPC IP31, Submissions 4-18 and 4-19).

Submission DP72-78: UPP 8(b) should be a separate Data Retention principle

Meaning of 'render non-identifiable'

The ALRC is of the view that the term 'permanently de-identify' should not be used in the UPPs and prefers the term 'render non-identifiable', because this makes it clear that agencies and organisations are obliged to take steps to prevent future re-identification of personal information (DP72, [25.85]). We agree, but submit that the term should be so defined in the Act, as its meaning is not obvious.

> ***Submission DP72-79: The Act should define 'render non-identifiable' as 'taking reasonable steps to prevent future re-identification of personal information'.***

'Retained' in this context means 'retained in identifiable form', so this principle (either UPP 8(b) or, as we suggest, a separate principle) can also be referred to generally as 'non-retention'.

Limiting justifications for retention

We previously submitted (CLPC IP 31, Submission 4-19.1) that the current formulation of NPP 4.2 allows organisations to justify retention on the basis of the myriad secondary purposes for which NPP 2 allows the information to be used and disclosed, whether or not they bear any relationship to the original purposes of collection. This is very dangerous. The single greatest protection for personal information against unexpected and unwelcome secondary uses, and against 'function creep' more generally, is to delete or de-identify it. If it no longer exists in identifiable form, it can no longer pose a risk to privacy. The increasing demands of law enforcement, revenue protection and intelligence agencies for personal information to be kept 'just in case' for their prospective access should be addressed through specific legal requirements, which can be debated and justified as clear exceptions to a general presumption of disposal. The ALRC has not discussed this issue in DP 72 and we submit that it should form a view in its final report, given the growing importance of data retention as a political and privacy issue. We adhere to our previous view.

> ***Submission DP72-80: The data retention principle (whether part of UPP 8 or separate) should provide that personal information must only be retained for any secondary purpose for which it has already legitimately been used, or for which there is express legal authority for retention. A Note should explain that secondary purposes for which personal information may be used or disclosed in future do not provide an alternative justification for retention***

Guidance on non-retention

The ALRC is proposing that the OPC should provide guidance about *when* it is appropriate for an agency or organisation to destroy or render non-identifiable personal information that is no longer needed for a purpose permitted under the UPPs (DP72, Proposal 25-5), and also *what is required* to achieve this, particularly when that information is held or stored in an electronic form (DP72, Proposal 25-6).

As discussed before, it is insufficient to merely *suggest* that OPC issue such guidelines.

Submission DP72-81: The OPC should be required by the Act to issue guidelines on the retention principle within one year.

We refer again to our general reservations about OPC Guidelines in our submission on the Commissioner's role (Response to DP72 Part F).

Destruction vs non-identifiability

The ALRC does not support giving an individual the general right to require an agency or organisation to destroy personal information it holds about the individual (DP72, [25.73]). Nor do its proposals indicate that destruction is to be preferred to non-identifiability. Nor would the guidelines discussed above require OPC to suggest when destruction is preferable.

It seems that the ALRC's position is that, provided 'non-identifiable' connotes permanence of de-identification, it is no different from destruction. However, the data may retain utility for statistical purposes. While we do not disagree with the ALRC's position to the extent of proposing an alteration, we question whether this matter has been examined sufficiently. In particular, there may be situations where the retention of non-identifiable data can lead to inferences being drawn (statistically) about a group of people. This may give members of that group of people legitimate reasons to prefer data destruction over non-identifiability.

Submission DP72-82: ALRC should give further consideration as to whether there are any circumstances where a person should be able to put forward a case for destruction rather than non-identifiability of their data.

11.4. Obligations of third party recipients

We support the ALRC's revised security principle making clearer than before that anyone who discloses personal information is obliged to take reasonable steps to ensure that it is protected against being used or disclosed by the recipient otherwise than in accordance with the UPPs.

However, there are two aspects of the ALRC proposal where it is not clear why the obligation is phrased narrowly, and a broader phrasing may be preferable. First, the expression 'discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation' is already quite broad, much broader than the normal understanding of 'contractors' (see CLPC IP 31, Submission 4-17, which was limited to contractors). There does not seem any obvious reason why this obligation should be limited in any way, except where a disclosure is required by law, in which case there will often be constraints on how far the discloser can impose conditions on the recipients (this should not prevent them from seeking to establish that the 'requiring' organisation or agency respects privacy rights as far as is consistent with their purpose. The obligation is in any event only to take 'reasonable steps', and should therefore be minimal when the risks are minimal.

Submission DP72-83: The obligation in UPP 8(c) should apply to all 'personal information it discloses to a third person'.

Second, it is not clear why the protection that the third party must provide is limited to protection to the information 'from being *used or disclosed* by that person otherwise

than in accordance with the UPPs' (emphasis added). It seems that the protection should at least extend to some other protections provided by the UPPs which are not covered by 'use or disclosure', including at least the requirement to observe UPP 8(a) (provide reasonable security). The discloser should not be required to take steps to ensure that recipients will observe obligations that properly only apply to them as independent data controllers, such as those concerning collection, quality, access, correction and deletion (assuming they are subject to an information privacy jurisdiction – if not then UPP 11 will apply and require additional steps).

Compliance with UPP 8(c) will require more than the discloser just satisfying itself that the recipient is subject to a privacy law – it must mean requiring from the recipient some demonstration of commitment to comply such as reference to a privacy policy? A discloser will have to ask at least 'what do you want the info for?' so how much more of a burden is it to add 'and how will you comply with privacy principles?'

> ***Submission DP72-84: The obligation in UPP 8(c) should extend to requiring third party recipients of personal information to observe all relevant UPPs in relation to that information.***

11.5. Data breach notification

We submit in 13.1 below that the data breach notification provisions proposed by the ALRC (DP72, Proposal 47-1) should be located in the UPPs, preferably as part of the security principle UPP 8.

12. Access and Correction (UPP 9)

12.1. Introduction and Application

The ALRC proposes a principle called 'Access and Correction' that (a) sets out the requirements that apply to *organisations* in respect of personal information that is held by organisations; and (b) contains a note stating that the provisions dealing with access to, and correction of, personal information held by *agencies* are located in a separate Part of the *Privacy Act* (DP72, Proposal 26-1).

We accept the ALRC's arguments for dealing with access and correction separately for agencies (where the relationship with the *FOI Act* is crucial) and organisations.

> ***Submission DP72-85: We support the inclusion in the UPPs of an access and correction principle (UPP 9) applying only to organisations.***

The proposed access and correction principle, like its counterpart NPP 6, has several different component parts – 9.1-9.7 plus two Notes

ALRC proposed UPP 9.1

> *9.1 If an organisation holds personal information about an individual and the individual requests access to the information, it must respond within a reasonable time and provide the individual with access to the information, except to the extent that:*
>
> *[Exceptions (a)-(j) follow – these are set out and discussed in turn below]*

12.2. Grounds for withholding

The ALRC proposes a number of grounds on which personal information can, at least initially, be withheld from an individual in response to an access request.

We generally support the proposed exceptions or 'grounds for withholding', with the following reservations:

Ground (a) – 'threat'.

> ***ALRC proposed UPP 9 exception (a)*** *providing access would be reasonably likely to pose a serious threat to the life or health of any individual;*

The ALRC proposes omission of the qualifying adjective 'imminent', in line with its proposals for UPPs 2 and 5. For the reasons we have given in our submissions on those principles, we opposed those changes, but in this instance we support the proposed change.

Ground (e) – 'revealing intentions'

> ***ALRC proposed UPP 9 exception (e)*** *providing access would reveal the intentions of the organisation in relation to negotiations with the individual in such a way as to prejudice those negotiations;*

This is potentially open to significant abuse through self-serving interpretations of 'intentions', 'negotiations' and 'prejudice'. We suggest that this ground be subject to a proportionality test.

Submission DP72-86: UPP 6.1(e) should be amended to add a second sentence: 'The extent of the refusal must be proportionate to the significance of the negotiations'.

Ground (g) – 'by or under law'

> ***ALRC proposed UPP 9 exception (g)*** *denying access is required or authorised by or under law;*

This needs to be amended to be consistent with the ALRC's proposal for the similar exception in UPP 5 (and elsewhere).

Submission DP72-87: UPP 6.1(g) should be amended to insert 'specifically' before 'authorised'.

Ground (i)– 'enforcement'

> ***ALRC proposed UPP 9 exception (i)*** *providing access would be likely to prejudice the:*
>
> *(i) prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or*
>
> *(ii) enforcement of laws relating to the confiscation of the proceeds of crime; or*
>
> *(iii) protection of the public revenue; or*
>
> *(iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or*
>
> *(v) preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;*
>
> *by or on behalf of an enforcement body; or*

This 'enforcement' exception is acceptable provided it is made clear that the condition 'by or on behalf of an enforcement body' applies to all five sub-grounds; requires the active involvement of an Australian enforcement body (as defined in the Act), and cannot be used to withhold information solely on the basis that there might subsequently be a referral to an enforcement body. Exception (h) is available for internal investigations of suspected unlawful activity.

Submission DP72-88: A Note should be added after UPP 6.1 to remind organisations that exception (i) requires the active involvement of an Australian enforcement body.

Other grounds

> ***Other UPP 9.1 exceptions proposed by the ALRC are:***
>
> ***(b)*** *providing access would have an unreasonable impact upon the privacy of other individuals;*
>
> ***(c)*** *the request for access is frivolous or vexatious;*
>
> ***(d)*** *the information relates to existing or anticipated legal proceedings between the organisation and the individual, and the information would not be accessible*

by the process of discovery in those proceedings;

(f) *providing access would be unlawful*

(h) *providing access would be likely to prejudice an investigation of possible unlawful activity;*

We support inclusion of these grounds for withholding, which are taken unchanged from NPP6, and do not appear to have caused any difficulty.

12.3. Evaluative information

ALRC proposed UPP 9.2

9.2 However, where providing access would reveal evaluative information generated within the organisation in connection with a commercially sensitive decision-making process, the organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: *An organisation breaches UPP 9.1 if it relies on UPP 9.2 to give an individual an explanation for a commercially sensitive decision in circumstances where UPP 9.2 does not apply*

We support the inclusion of a special provision (UPP 9.2) dealing with access to evaluative information, but it is important to ensure that this is not used to override direct access where that is appropriate. One example – credit scores – is addressed specifically in relation to Chapter 55 (DP72, Proposal 55-3) and Proposal 7.5(d) addresses the issue of other types of information (such as unintelligible algorithms) which may also require special consideration when responding to access requests.

The Note proposed to follow 9.2 does not in our view add anything – it is tautologous.

Submission DP72-89: The Note after UPP 9.2 should be replaced by one advising that 'The mere fact that some explanation may be necessary in order to understand information such as a score or algorithm result should not be taken as grounds for withholding information under 9.2.'.

12.4. Access through Intermediaries

ALRC proposed UPP 9.3

9.3 If the organisation is not required to provide the individual with access to the information because of one or more of paragraphs UPP 9.1(a) to (j) (inclusive), the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that the compromise would allow for sufficient access to meet the needs of both parties.

The ALRC proposes that where an organisation is not required to provide an individual with access to his or her personal information because of an exception to the general provision granting a right of access, the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, provided that would allow for sufficient access to meet the needs of both parties (DP72, Proposal 26-2).

We support the basic proposition, but suggest that the qualification 'provided that would allow for sufficient access to meet the needs of both parties' could become an obstacle to compromise rather than facilitating it. It will often be the case that neither party will be satisfied by a compromise but this is no reason not to provide for it.

> ***Submission DP72-90: UPP 9.3 should be amended to replace 'provided that would allow for sufficient access to meet the needs of both parties' with 'to allow for access to at least some of the information.'***

We suggest that the Privacy Commissioner be empowered to act as an intermediary either if the parties request it or in the event that they are unable to agree on an alternative.

> ***Submission DP72-91: UPP 9.3 should be amended to add 'In the absence of agreement, the Privacy Commissioner would be the intermediary.' The Privacy Commissioner should be empowered to act as an intermediary in the context of UPP 9.3.***

The ALRC further proposes that the OPC should provide guidance about the meaning of 'reasonable steps' in the context of reaching an appropriate compromise. This guidance would make clear, for instance, that an organisation need not take any steps where this would undermine a lawful reason for denying a request for access in the first place (DP72, Proposal 26-2).

We support this proposal, subject to our general comments elsewhere on OPC guidance.

We are also concerned that organisations do not use the existence of grounds for withholding some information as an excuse for denying access requests in their entirety. This has proved to be a constant problem in the operation of Freedom of Information laws – even with government agencies that are supposedly under direction to comply with the spirit of openness. It is unrealistic to expect private sector organisations to be any more generous in their approach to access rights, and firm guidance is required (in association with vigorous enforcement – see our submission on DP72, Part E)

> ***Submission DP72-92: The Office of the Privacy Commissioner should be expressly required to issue guidance to the effect that organisations should only claim any relevant exceptions (grounds for withholding) to the minimum extent necessary and that they should wherever possible provide as much of the information held as possible, even if this means selective editing or suppression of material subject to one of the exceptions.***

12.5. Barriers to Access: Fees and Timeframe

ALRC proposed UPP 9.4

> *9.4 If an organisation charges for providing access to personal information, those charges:*
>
> *(a) must not be excessive; and*

(b) must not apply to lodging a request for access.

The ALRC proposes that UPP 9 should require an organisation to respond within a reasonable time to a request from an individual for access to personal information held by the organisation. The Office of the Privacy Commissioner should provide guidance about the meaning of 'reasonable time' in this context (DP72, Proposal 26-3).

UPP 9.4 allows organisations to charge for access but provides that any charges must not be excessive and that they must not apply to simply lodging a request. The ALRC is of the view that it is not desirable to provide further legislative guidance as to fees for accessing personal information (DP72, [26.29]).

We support the inclusion of UPP 9.4 but suggest that some binding benchmarks be provided on both response times and fees.

Submission DP72-93: Either Regulations or a binding Code should set benchmarks for response times and fees in relation to access and correction requests.

12.6. Correction of Personal Information

ALRC proposed UPP 9.5

9.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, the organisation must take reasonable steps to:

(a) correct the information so that it is accurate, complete, up-to-date and relevant; and

(b) [see below]

The ALRC proposes that an individual should have to 'establish' that personal information held by an organisation is incorrect before the organisation is obliged to correct the information (DP72, [26.38] and UPP 9.5(a)).

We submit that it is too onerous to place the entire burden of evidence on the individual seeking to make a correction. We suggest a qualified test.

Submission DP72-94: UPP 9.5 should be amended to read 'to establish on the balance of probabilities …'

The proposed UPP 9.5 includes the qualification 'with reference to a purpose of collection permitted by the UPPs.' We submit that this potentially allows an organisation to decline correction on the grounds that while the information may be incorrect (i.e. inaccurate, incomplete, out of date and/or irrelevant) in relation to the actual purpose for which the information in question was collected, it is not 'incorrect' in relation to *another* of their purposes. This is clearly neither fair nor acceptable. We refer to the similar point we have made in relation to UPP 8.2.

Submission DP72-95: UPP 9.5 should be amended to read 'with reference to the purpose(s) for which the information was collected.'

The proposed principle offers no guidance about the various ways in which information can be corrected, and about the tension between correction and archiving (information integrity) principles – sometimes embodied in other laws.

Submission DP72-96: The Privacy Commissioner should be required to issue guidance to the effect that correction can take the form of amendment, deletion or addition, as appropriate in the circumstances. The guidance should also advise that there are many situations where there is a legal requirement to keep an historical record of actual transactions, but that this should not prevent the correction of 'operational' records, leaving the original incorrect information only in an archive.

Notifications of previous errors

ALRC proposed UPP 9 also provides as follows:

> *9.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, the organisation must take reasonable steps to:*
>
> *(a) [see above]*
>
> *(b) notify any other entities to whom the personal information has already been disclosed prior to correction, if requested to do so by the individual and provided such notification would be practicable in the circumstances.*

The ALRC proposes that that where, in accordance with this principle, an organisation has corrected personal information it holds about an individual, and the individual requests that the organisation notify any other entities to whom the personal information has already been disclosed prior to correction, the organisation must take reasonable steps to do so, provided such notification would be practicable in the circumstances (DP72, Proposal 26-4 and UPP 9.5(b)).

We support Proposal 26-4 for the inclusion of UPP 9.5(b).

However, we can also see circumstances in which it should apply other than where the individual requests it – e.g. where the organisation becomes aware of errors in other ways. We accept that there will be some circumstances in which notification of previous recipients would be either impracticable and/or against the interests of the individual, so we do not suggest notification be the default. However, we can also envisage circumstances in which an organisation may become aware of errors without the individual concerned knowing about them, and where notification of specific previous recipients could be very much in the individual's interests. The best solution is probably not to have any requirement to notify previous recipients, but rather a requirement to notify the data subject, who can then choose whether they wish to exercise their right (under Proposal 26-4 above) to have previous recipients notified. This is consistent with the ALRC's approach in Proposal 26-4. The only difficult question is to define the type of 'correction' of a person's record which should trigger the necessity for notification. Minor corrections such as the spelling of a person's

name or a detail of their address should not do so. The trigger should be more like 'correction of personal information under circumstances where there is a reasonable likelihood that the previous information has had an adverse effect on the interests of the person'.

Such an obligation to notify the individual could be located in UPP 9, or in the data quality principle (UPP 7), or even integrated with the proposed data breach notification right..

> ***Submission DP72-97: Where an agency or organisation makes a correction to personal information about a person which has previously been used or disclosed under circumstances which is reasonably likely to have had an adverse effect on the person, they should inform the person of the correction and of any such previous disclosures of the information. Such an obligation could be located in UPP 7, UPP 9 or integrated with the proposed new data breach notification obligation wherever that is located.***

Statements re disputed content

ALRC proposed UPP 9.6

> *9.6 If the individual and the organisation disagree about whether the information is, with reference to a purpose of collection permitted by the UPPs, not accurate, complete, up-to-date and relevant, and the individual asks the organisation to associate with the information a statement claiming that the information is not accurate, complete, up-to-date or relevant, the organisation must take reasonable steps to do so.*

The ALRC prefers the word 'associate' (in NPP 6) to 'attach' (in IPP 7) where there is a disagreement about accuracy and the individual asks the organisation to 'associate with the information a statement…'(DP72, [26.37] and UPP 9.6).

We support the wording of UPP 9.6, subject to the following reservation and suggested addition.

In our earlier submission, we drew attention to the issue of ensuring that any 'notes' made in response to disputed information are stored in such a way that they are visible to subsequent users, whether internal or in recipients after a disclosure (CLPC IP31 Submission 4-25.3).

We are aware of practical difficulties in doing this in the context of automated credit reference systems (see our submission on DP72 Part G, Chapter 54). However, we submit that there should be a general obligation to this effect – otherwise the value of a right to have notes added about disputed information would have to be seriously questioned.

> ***Submission DP72-98: UPP 9.6 should specify that the obligation in relation to disputed information has to be performed in a way which ensures that any annotation is made available to any subsequent user of the disputed information.***

12.7. Reasons for denial

ALRC proposed UPP 9.7

> *9.7 An organisation must provide reasons for denial of access or a refusal to correct personal information.*

We support the ALRC proposal for a requirement to give reasons for denial of access or refusal to correct (UPP 9.7). However, the obligation needs to be more specific in requiring an organisation to specify *which* of the exceptions it has relied on to deny access or correction. It should also be made clear in guidance that denial of access can only be based on the grounds specified at the time – it should not be open to an organisation to later rely on alternative grounds.

> ***Submission DP72-99: UPP 9.7 should be amended to add a second sentence: 'The reasons should specify which of the exceptions in UPP 9 apply.' The OPC should issue guidance on the application of this sub-principle.***

12.8. Notification of Access Rights

The ALRC believes that specific notification of access rights is not required in the UPP 9 as it is already covered by the proposed 'Specific Notification' and 'Openness' principles (UPPs 3 & 4) (DP72, [26.60])

We support this position.

13. Identifiers (UPP 10)

13.1. Introduction

The ALRC is proposing to extend the principle governing use of identifiers developed by other organisations, by expanding the scope of what counts as an identifier. It also proposes to apply the principle to Federal Government agencies whereas previously it only applied to the private sector.

ALRC proposed UPP 10 - Identifiers

10.1 An organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency;

(b) an agent of an agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.2 An agency must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) another agency;

(b) an agent of another agency acting in its capacity as agent;

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract; or

(d) an Australian state or territory agency.

10.3 The requirements in NPPs 10.1 and 10.2 do not apply to the adoption by a prescribed agency or organisation of a prescribed identifier in prescribed circumstances.

Note: *There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2), as proposed to be amended.*

10.4 Where an identifier has been 'assigned' within the meaning of UPP 10.1 or 10.2, an agency or organisation must not use or disclose the identifier unless:

(a) the use or disclosure is necessary for the agency or organisation to fulfil its obligations to the agency that assigned the identifier;

(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure;

(c) the identifier is genetic information and the use or disclosure would be permitted by the proposed Privacy (Health Information) Regulations; or

(d) the use or disclosure is by a prescribed agency or organisation of a prescribed identifier in prescribed circumstances.

10.5 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or any other particular that:

(a) uniquely identifies an individual for the purpose of an agency's or organisation's operations; or

(b) is determined to be an identifier by the Office of the Privacy Commissioner. However, an individual's name or ABN, as defined in the A New Tax System (Australian Business Number) Act 1999, *is not an 'identifier'.*

Note: *A determination referred to in the 'Identifiers' principle is a legislative instrument for the*

purposes of section 5 of the Legislative Instruments Act 2003 *(Cth).*

13.2. Scope of regulation of identifiers

We support the ALRC's proposal that the UPPs should contain a separate principle that regulates identifiers (DP72, [27.17]), and that it should be equally applicable to agencies (essentially, the federal public sector) and organisations (DP72, [27.23]) but with appropriate exceptions (DP72, [27.28]). As a result, s100(2) and (3) of the *Privacy Act* should also be amended to apply to agencies.

We support Proposal 27-1 for a separate 'Identifiers' principle to apply both to agencies and to organisations.

Definition of 'identifier'

We agree with the ALRC's view that including the words 'a symbol or any other particular' in the definition of 'identifier' would be a useful way to ensure that biometric and other non-numerical identifiers are treated as identifiers (DP72, [27.44]) and we therefore support Proposal 27-2.

We agree that, where a number, symbol or any other particular does not of itself *uniquely* identify an individual, the OPC should be empowered to make a determination that the number, symbol or particular is still an 'identifier' for the purposes of the 'Identifiers' principle in the proposed UPPs (DP72, [27.44] and Proposal 27-2), and that such a determination should be a legislative instrument and so disallowable (DP72, [27.45] and Proposal 27-3).

We support Proposals 27-2 and 27-3.

The ALRC does not seem to make a distinction between "identification" and "authentication"/"verification". The term "identifier" appears primarily if not solely to apply to schemes involving identification (i.e., distinguishing a person from a group) rather than authentication (i.e., showing that someone is who they claim to be). However, some biometrics are presently applied for purposes of authentication rather than identification. Thus, it cannot be assumed that the term "identifier" as apparently defined here will capture all biometrics schemes.

> ***Submission DP72-100: The definition of 'identifier' should also encompass when identifiers are used for authentication (verification) and not only when used for identification.***

Exception by regulation

We do not agree with the special powers to make exceptions by regulation in UPP 10.3 (which erroneously refers to 'NPP's) and 10.4(d). The appropriate way for such exceptions to be made is by public interest determinations, where proposals for exceptions will undergo appropriate scrutiny and opportunities for public input which are not provided by a regulation-making power.

> ***Submission DP72-101: UPP 10.3 and UPP 10.4(d) should be deleted, and any exceptions left to the public interest determination process.***

13.3. Content of the identifiers principle

We support the ALRC's suggestions that:

- Data-matching is not inherently linked to the use of identifiers, so data-matching should be subject to regulation in addition to this principle (DP72, [27.50]).
- The arrangement for collection and disposal of identifiers are adequate and covered by other proposed UPPs such as collection and data security, as well as other sections of the *Privacy Act* (DP72, [27.53]).
- An exception that would allow individuals to consent to the use and disclosure of identifiers should not form part of the principle, as it would be inconsistent with its function (DP72, [27.64]).

We also support the ALRC's proposal that

- UPP 10 should regulate the use by agencies and organisations of identifiers that are assigned by state and territory agencies (DP72, Proposal 27-4).

Submission DP72-102: We support the application of UPP 10 to identifiers that are assigned by state and territory agencies

13.4. Unique multi-purpose identifiers

Multi-purpose identifiers pose particular dangers to privacy and need more rigorous control than single-purpose identifiers. We previously submitted that

> The privacy principles in the *Privacy Act*, and methods for adjudication concerning breaches of them, should apply to any unique multi-purpose identifiers adopted in Australia. Any variations from the application of any of the principles should be defined by specific legislative provisions stating exceptions or variations, and not left to inference from the existence of a different set of principles. Such an approach will (i) ensure that variations are obvious; (ii) facilitate a consistent body of law emerging on both the core principles and the exceptions. [see CLPC IP31 Submission 12-3]

We support the ALRC's suggestion that any exceptions to UPP10 should be clearly set out in legislation establishing multi-purpose identifier schemes (DP72, [27.110]) – this should be made a firm proposal/recommendation.

The ALRC proposes that, before the introduction by agencies of any unique multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should consider the need for a privacy impact assessment (DP72, Proposal 27-5). This allows for far too little public input or disclosure, and is liable to be both skewed by the terms of reference or choice of consultant to ensure that key questions are not asked, or hidden if the results are not to the government's liking, as recent examples have demonstrated (see our submission on PIAs generally in our response to Part F of DP72).

Submission DP72-103: The Act should require that, before the introduction by agencies of any unique multi-purpose identifier, an independent and public privacy impact assessment should be commissioned, the terms of reference of which should be a determination by the Privacy Commissioner,

such a determination being a legislative instrument. Any exceptions to UPP10 should be clearly set out in legislation.

We agree with the ALRC's view that the number on the 'access card' proposed by the previous government would have been likely to fall within the definition of 'identifier' (DP72, [27.109]). So too would the underlying registration number, which would have been even more of a risk to privacy than the card number.

Regulation of Tax File Numbers (TFNs)

Consistent with its overall approach to identifiers, ALRC proposes that OPC, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the *Tax File Number Guidelines* issued under s 17 of the *Privacy Act* (DP72, Proposal 27-6). We previously submitted that the TFN should be dealt with consistently with other multi-purpose identifiers (CLPC IP31, Submission 12-1), and therefore support this proposal. We note that elsewhere the ALRC recommends that binding guidelines be renamed 'rules' (DP72, Proposal 44-2).

Submission DP72-104: OPC should be required by the Act to review within one year the Tax file number (TFN) Guidelines (Rules) so as to make them consistent with UPP 10.

14. Transborder Data Flows (UPP 11)

14.1. Introduction

The ALRC proposes that the 'data export' provisions be strengthened so that organisations (and Commonwealth government agencies) would have to remain liable for the handling of personal information sent overseas if they wished to take advantage of many of the grounds justifying data exports.

The ALRC also proposes that the Australian government should publish a 'white list' of countries with laws providing similar protection to Australian laws. This would make it easier to assess whether a data exporter reasonably believed that another country had similar laws to Australia. This is not a path down which governments or Privacy Commissioners in other countries have been eager to tread, as the stakes are very high in terms of the potential effect on trade and inter-governmental relations.

14.2. Scope of the prohibition on overseas transfers

ALRC proposed UPP 11 - Transborder data flows

> *An agency or organisation in Australia or an external Territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia only if:*

The use of 'only if' effectively creates four exceptions[8] to transfers outside Australia.

> *[Exceptions (a) – (d) below follow]*

We support the ALRC proposals that UPP 11 should apply to both agencies and organisations (DP72, Proposal 28-2, and the consequential Proposal 28-1). We also support the suggestions that it should refer to the transfer of personal information to a 'recipient' rather than 'someone' (DP72, [28.44]); and that it should refer to transfers 'outside Australia' rather than to a 'foreign country' (DP72, [28.44]).

Online information

The ALRC asks:

> *Question 28-1(a): Should the Privacy Act provide that for the purposes of the proposed 'Transborder Data Flows' principle, a 'transfer' (a) includes where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia; and*

Unless 'making available' personal information to overseas users is considered to be a transfer, all data export provisions can be avoided. It does not matter whether the material is accessible by everyone, or only by those with a password, or whether the data is encrypted. The exclusion of 'publicly available information' from the meaning of 'personal information' will mean that information placed on the Internet which can legitimately be disclosed can also legitimately be transferred overseas.

---

[8] The construction of UPP 11 has four 'conditions' for transfer (i.e. 'only if'), but we consider it more helpful to discuss them as 'exceptions' to the principle of a prohibition on transfer (i.e. 'not unless') – this is more consistent with the construction of other UPPs – in particular UPP 5

While it is clear that the general principle is correct that 'disclosure via Internet' should be a transfer, there may be some situations where disclosure of personal information for non-business and non-government purposes would be allowed, as a disclosure (i.e. within Australia) and does not do any harm as a transfer (i.e. via Internet and therefore outside Australia). However UPP 11 does not yet adequately provide for this because it is oriented toward business and government transfers. The ALRC should consider this and look at how the situation has been dealt with in Sweden where this issue first arose in the EU. If it is too difficult to anticipate what exceptions may arise, but there is desire to avoid punitive results in trivial situations, an exception-making power may be justified, limited to the non-business and non-government context.

> ***Submission DP72-105: 'Transfer' should include where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia. However, the ALRC should consider whether as a result any additional exception allowing some transfers in non-business and non-government settings should be made.***

'Temporary' transfers

> *Question 28-1(b): Should the Privacy Act provide that for the purposes of the proposed 'Transborder Data Flows' principle, a 'transfer' (b) excludes the temporary transfer of personal information, such as when information is emailed from one person located in Australia to another person also located in Australia, but, because of internet routing, the email travels (without being viewed) outside Australia on the way to its recipient in Australia?*

We consider that a 'transfer' should occur if and only if there is a recipient outside Australia who uses or stores the information for purposes other than merely communicating it to its final recipient. Communication of data by routes such that it is intercepted by parties outside Australia should constitute a transfer, and thus be able to be prevented because it is a breach of UPP 11 (unless, of course, the transfer to that recipient is covered by one of the exceptions (a)-(d)). Allowable transfers should only be as temporary as the necessities of the communication allow, and should not include situations where storage overseas is required by law or is otherwise practised for any other reason. If transfers involving retention periods are involved, this should be a transfer covered by UPP 11 and requiring justification under one of the other exemptions.

> ***Submission DP72-106: A 'transfer' should only occur if there is a recipient outside Australia who uses or stores the information for purposes other than communicating it to its final recipient. Communications may involve temporary storage, but if the information is subject to set retention periods whether required by law or otherwise, there will be a transfer.***

Transfers to other domestic jurisdictions

We note that the ALRC appears to have accepted without question that the transborder principle should, as NPP 9 does now, only apply to transfers to foreign countries/outside Australia (DP72, [28.42-28.44]).

We believe that a case could easily be made for applying the Principle also to transfers to other jurisdictions within Australia. There are currently several States which do not have privacy laws applying to their public sector, and even those which do should arguably be subject to an assessment as to whether their principles are 'substantially similar' (to use the words of proposed exception (a)). Why should an organisation or agency not have to satisfy one of the exceptions in UPP 11 in order to be able to transfer personal information to a State government agency? The ALRC notes (but without comment on the implications) that the WA, Victorian and NT privacy laws all contain a transborder data transfer principle that applies to transfers *outside their own jurisdiction*; i.e. including to other Australian States and Territories (DP72, [28.33]).

This issue is likely to be relevant to any consideration by other jurisdictions as to the adequacy of Australian privacy laws – this is discussed further below.

14.3. The four exceptions allowing overseas transfers

We suggest that the ALRC explains more clearly in its final report how UPP 11 relates to and interacts with UPP 5. Every overseas transfer must also be either a use (if internal to an organisation or agency) or a disclosure (if to a third party) and the organisation or agency must therefore also satisfy UPP 5. The UPP 11 exceptions are an additional hurdle that must be crossed where an overseas transfer is involved. Given this relationship, why does UPP 11 need to replicate some of the UPP 5 exceptions? We highlight this issue where it arises in the context of the individual UPP 11 exceptions.

ALRC proposed UPP 11- Exception (a) 'reasonable belief' and 'whitelist'

This exception to UPP 11 allows transfers where:

> *(a) the agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the UPPs; or*

The ALRC does not propose the amendment of the 'reasonable belief' test currently found in NPP 9(a).

Instead, the ALRC proposes that the Australian Government should develop and publish a 'whitlelist' ('a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to the proposed UPPs') (DP72, [28.49]).

We support the ALRC's proposal that there should be a 'whitelist' of such 'substantially similar' protections published (CLPC IP 31, Submission 13-3; DP72, Proposal 28-8). There is little point in pretending that such a whitelist would not automatically qualify as a basis for 'reasonable belief', so the 'whitelist' may as well be by regulation stated to have that effect. However, for reasons discussed below in relation to APEC and similar matters, there is considerable danger of abuse if such a power is put into the hands of a government with no checks against its misuse. We therefore propose two such checks: (i) any regulation should only be able to be made after the receipt of published advice by the Privacy Commissioner; and (ii) the

whitelist should be made by legislative instrument, so as to open it to Parliamentary scrutiny and disallowance.

> ***Submission DP72-107: Any 'whitelist' in relation to UPP 11(a) should be by a regulation or other legislative instrument made by the government, and made after receipt of published advice from the Privacy Commissioner.***

The proposed exception requires the overseas 'scheme' to '*effectively* uphold privacy protections…' (emphasis added). The ALRC argues that in these circumstances an individual can seek redress overseas. We suggest that this is unrealistic in that private individuals cannot be expected to have the necessary skills, knowledge and resources to seek redress successfully on their own. In our view it is essential that for a foreign scheme to be judged as eligible for the whitelist, there must be an agreement in place between the Privacy Commissioner and appropriate regulators in the other jurisdiction, to facilitate complaint investigation and cross-border enforcement. The Privacy Commissioner already has such an agreement with the NZ Privacy Commissioner, and similar arrangements are one of the priorities for implementation of the APEC Privacy Framework.

> ***Submission DP72-108: In order to qualify for the 'whitelist' for the purposes of UPP 11(a), a foreign jurisdiction must have in place an agreement on cross border enforcement with the Australian Privacy Commissioner.***

In the ALRC's view, agencies and organisations should not remain accountable when they reasonably believe that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the proposed UPPs (DP72, [28.70]).

In our view, in the absence of any such clear expression of public policy in the form of a 'whitelist' legislative instrument, there is no justification for privileging mere subjective belief of the data exporter by releasing them from all breaches of the UPPs which are subsequently committed by the overseas recipient or others. Why should the person whose privacy has been infringed be forced to take legal proceedings in a foreign jurisdiction? Instead, as we have argued previously, the exporter should remain liable, as in exception (d)(CLPC IP 31, Submission 13-1).

> ***Submission DP72-109: Except where a transfer is to a jurisdiction included in a 'whitelist' legislative instrument, the agency or organisation should continue to be liable for any breaches of the UPPs (as in exception (d)).***

ALRC proposed UPP 11- Exception (b) 'consent'

This exception to UPP 11 allows transfers where:

> *(b) the individual consents to the transfer; or*

We previously criticised NPP 9 on the basis that consent for transfer does not have to be 'unambiguous' (to use the EU's term).

For most purposes in the Act 'consent' is defined to include implied consent. For example, UPP 5 can be satisfied if the individual (concerned) has consented to the use

or disclosure (exception (b)). With the proposed exception (b) to UPP 11, implied consent could satisfy both UPP 5 and UPP 11 at the same time. We believe that in the context of overseas transfers, with its major potential for loss of privacy protection, organisations and agencies should not be able to rely on implied consent.

> ***Submission DP72-110: UPP condition (b) should require that the individual 'expressly' consents to the transfer.***

Another major flaw in the proposed consent exception is that the ALRC anticipates that it would relieve the agency or organisation from any liability for how the information is handled overseas. This approach completely overlooks the fact that individuals will typically have absolutely no capacity to sensibly assess the risks associated with transborder data flows.

In our view, the consent exception should be conditional upon the person having been given notice of (i) *which* country or countries the data will go to and (ii) the fact that the transferor will no longer be liable for any breaches since the ALRC proposes that this exception should be an alternative to exception (d) (DP72, [28.69]). Without these two pieces of information, consent is not 'informed'.

Given that under our preferred exception, express consent will be required, there can be no argument about notice of these matters being impracticable. We argue below (and in relation to UPP 3) that there should be a general requirement as part of UPP 3 for notification of specific countries, and this would satisfy the first additional condition for exception (b). However, specific notice that the transferor will no longer be liable for any breaches only makes sense in the specific context of reliance on exception (c) and should therefore form part of UPP 11.

Even where the consent exception applies, we believe the transferor should remain subject to the general obligation – currently only in exception (d)(v) – to take reasonable steps to ensure compliance with the UPPs or similar standards – we return to this in our submission on exception (d) below.

> ***Submission DP72-111: UPP 3 should provide for the individual concerned to be given notice of the specific country or countries to which the data may be transferred. The consent exception (b) in UPP 11 should be conditional on (i) compliance with this aspect of UPP 3, and (ii) notice when obtaining express consent of the fact that the transferor will no longer be liable for any breaches. The consent exception should also be conditional upon the obligation in UPP 11 (d)(v).***

ALRC proposed UPP 11- Exception (c)

This exception to UPP 11 allows transfers where:

> *(c) the transfer is necessary for one or more of the following by or on behalf of an enforcement body*
>
> *(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;*
>
> *(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;*

> *(iii) the protection of the public revenue;*
>
> *(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;*
>
> *(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;*
>
> *(vi) extradition and mutual assistance; or*

We are reluctant to support this law enforcement exception.

The wording of this exception is similar to exception (f) in UPP 5, but with two differences. Firstly, it is more objective in requiring the transfer to be 'necessary' rather than simply a reasonable belief of necessity. Secondly, it adds 'extradition and mutual assistance'.

We note that the definition of 'enforcement body' in the Act means that this exception requires the involvement of one of the *Australian* agencies covered by that definition. An overseas enforcement agency could not ask an Australian organisation or agency to disclose personal information under this exception without going through an Australian enforcement body.

We also note that the ALRC sees this exception as meaning that no 'required or authorised by or under law' exception (with or without the addition of 'specifically' as discussed elsewhere) is necessary. This is consistent with the current NPP 9 which contains no 'required or authorised by or under law' exception.

However, the 'downside' of a general 'assistance to enforcement agencies' exception is that it potentially allows for transfer to a wide range of bodies in jurisdictions not only lacking in privacy protection rules, but also lacking in basic standards of legitimacy, human rights or natural justice. It may be that some protection would be afforded by other obligations of Australian enforcement bodies that would have to be involved in any transfer under this exception. Yet without assurances to this effect, we are reluctant to support this proposed exception. At the very least, agencies and organisations transferring under this exception should be required to seek assurances about privacy protection – i.e. exception (d)(v) should apply.

It is not clear why it this exception is more permissive is some key respects than the equivalent exception in UPP 5, or how it would interact in practice with that exception. In our view any foreign transfer for enforcement purposes requires additional, not fewer safeguards.

> ***Submission DP72-112: Any 'enforcement' exception to UPP11 must be more tightly worded and conditional.***

ALRC proposed UPP 11- Exception (d) where the transferor continues to be liable

This exception to UPP 11 allows transfers where:

> *(d) the agency of [sic - assume 'or'] organisation continues to be liable for any breaches of the UPPs, and*
>
> *(i) the individual would reasonably expect the transfer, and the*

transfer is necessary for the performance of a contract between the individual and the agency or organisation;

(ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request;

(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party;

(iv) all of the following apply: the transfer is for the benefit of the individual, it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or

(v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the UPPs.

***Note:** Agencies and organisations are also subject to the requirements of the 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside*

We previously proposed that 'data exporters should remain liable for breaches of standards by data importers under most circumstances' (CLPC IP 31, Submission 13-1). The ALRC has adopted this approach in relation to exception (d), which includes the majority of the previous exceptions to NPP 9. This is a very significant change, which we support. The retention of liability by the exporter makes the breadth of the exceptions allowing export less important (though still significant). Conditions (d)(i)-(iv) are in any event not so contentious, being similar to those in Art 26(1) of the EU Data Protection Directive.

We previously criticised NPP 9 exception (e) [now UPP (d)(i)] on the basis that organisations are allowed to make an assumption about the likelihood of consent where it is impracticable to obtain it. The ALRC proposes that UPP 11 (d)(i) and (ii) require that the transfer of personal information overseas should be within the reasonable expectations of the individual. We support this change. In the ALRC's view, organisations and agencies wishing to rely on this exception should be required to specify in a contract or in pre-contractual arrangements that the fulfilment of the contract may require the overseas transfer of an individual's personal information. (DP72, [28.53]). The 'reasonable expectation' provision will make it more likely that organisations and agencies will make the likelihood of overseas transfers subject to explicit notice. (Note that we have also submitted that this be an express condition of exception (b)).

The ALRC does not propose the removal of the requirements in NPP 9(d) and (e) – now proposed as (d) (iii) & (iv) of UPP 11 – that a contract is in the 'interest of the individual' or that the transfer is for the 'benefit of the individual' (DP72, [28.56]). The ALRC acknowledges, however, that these requirements involve subjective assessments. To assist agencies and organisations in making these assessments, the ALRC suggests that the OPC develop and publish guidance on the proposed UPP 11, addressing when a transfer of personal information is for the benefit or in the interests of the individual concerned (DP72, [28.56]). In the ALRC's view, where the reason for a transfer is organisational efficiency alone, the transfer should only take place if

one of the other conditions in the proposed 'Transborder Data Flows' principle is satisfied (DP72, [28.57]). We support these suggestions, subject to our general comments about OPC guidance (see our submission on DP72 Part F).

The ALRC suggests that NPP 9(f) – now the proposed UPP 11 (d)(v) – be amended to require that *before* a transfer takes place, an agency or organisation must take reasonable steps to ensure that the information will not be handled by the recipient of the information inconsistently with the proposed UPPs (DP72, [28.61]). As we pointed out in our criticisms of NPP 9, that principle probably does not even require that the individual should have some recourse against anyone in the event that the 'reasonable steps' turn out to be inadequate, and this is much weaker than the Directive. The UPP 11 proposals remedy this, and we support them.

The ALRC proposes that guidance on the proposed UPP 11 should include advice on what constitutes 'reasonable steps' which only appears in UPP 11(d)(v) (DP72, [28.61]), and we support this.

However, we cannot see why the UPP 11(d)(v) requirement (previously NPP 9(f)) – to take reasonable steps to ensure that information will not be dealt with by the recipient inconsistently with the UPPs) should be seen as an *alternative* basis for transfer, even where the transferor remains liable for breaches. In our view, (d)(v) should be a condition applying to all transfers on the basis of (d)(i)-(iv), as well as to transfers on the basis of consent (exception (b)), and by or on behalf of enforcement bodies (exception (c) – subject to our comments above) – as already suggested above.

The 'reasonable steps' required to satisfy (d)(v) in many cases would not be onerous – but we can see no reason why transferors should not, as a minimum, seek assurances from the recipient that they will observe the UPPs or an equivalent.

> ***Submission DP72-113: In UPP 11, condition (d)(v) should apply to all transfers on the basis of (d)(i)-(iv), as well as to transfers on the basis of consent (exception (b)), and by or on behalf of enforcement bodies (exception (c)).***

14.4. Requirement of notice of data exports

In the ALRC's view, requiring notification or written consent each time an agency or organisation transfers an individual's personal information overseas would result in an unjustified compliance burden (DP72, [28.118]). The ALRC noted that the specific notification principle would extend to an individual if his or her personal information might be transferred outside Australia (DP72, [28.119]). Also, the Privacy Policy of an agency or organisation, referred to in the proposed 'Openness' principle, should set out whether personal information may be transferred outside Australia (DP72, Proposal 28-10). We support this but go further.

As mentioned in our previous submission, a requirement to notify would be one of the most effective protections against inappropriate transfers. It should extend to notification of *which* jurisdiction data is to be transferred, and the identity of the recipient in that jurisdiction. It will assist individuals to exercise informed choice and/or bring pressure to bear for improvements in legislative protection, at least in Australian jurisdictions without adequate laws.

We have already argued above for this specific notification to be made a condition of the consent exception in UPP 11(b), and repeat the suggestion that it also be made a more generic requirement of UPP 3.

> ***Submission DP72-114: There should be a requirement to inform individuals that their personal information is to be transferred to any jurisdiction without equivalent privacy protection (including some State jurisdictions within Australia). If the organisation has an intention to transfer at the time of collection, it should give notice at that point. If it later decides to export the data, it should give notice at that time.***
>
> ***Submission DP72-115: There should also be a requirement to inform individuals of the jurisdiction(s) to which their personal information is to be transferred, and the identity of the recipient(s) in the(se) jurisdiction(s).***

14.5. International privacy protection

Comparison with international standards – Europe

The ALRC makes a number of proposals in DP 72 which, if enacted, may assist an 'adequacy' finding under the EU privacy Directive, including the removal of the small business exemption and the employee records exemption; clarification of the 'required or authorised by or under law' exception; and (to some extent) strengthening of UPP 11, including the development of a 'whitelist' in relation to it (DP72, [28.150]). The proposed changes in UPP 11 (from NPP 9) would also make it more likely that a finding of 'adequacy' would be made.

Minimal relevance, and dangers, of the APEC Privacy Framework

The ALRC is of the view that the involvement of Australia in the implementation of the APEC Privacy Framework will not require the lowering of any privacy protections under the *Privacy Act*.

For reasons set out in our previous submission, we substantially agree (CLPC IP31 Submission, p. 86). However, as already noted, we have reservations about the ALRC's suggestion that the Australian Government should decide which countries' 'laws and binding schemes' should be on the 'whitelist' for the purpose of UPP 11 (DP72, [28.49]). Such a listing will in effect exempt all transfers to a whitelisted country from UPP 11. The possibility that this whitelisting could be abused to unjustifiably include some countries involved in the APEC Privacy Framework – particularly certain allies of Australia and its largest trading partners – is real and substantial and should not be ignored by the ALRC. The EU's contentious acceptance of the 'adequacy' of the US 'Safe Harbor' system, despite the serious reservations of its own privacy regulators, is notorious evidence of such abuse.

It is primarily the danger of 'APEC abuse' that compels us to propose that any whitelisting, while still valuable in relation to the effectiveness of UPP 11, must be both by regulations and with the published agreement of the Privacy Commissioner.

The ALRC considers that the APEC Privacy Framework may provide new ways of encouraging compliance with local and international privacy standards (DP72, [28.178]). We agree that it could, even though progress in this respect has, to date,

been minimal – the programme of 'Pathfinder projects' agreed at the APEC summit in September 2007 is intended to further this objective.

Proposed accession to the Council of Europe Convention 108

Another international standard which should be given serious consideration as an appropriate model for the protection of personal information transferred between countries is the Council of Europe's privacy Convention (Council of Europe 1981). In their 2005 *Montreux Declaration* the world's privacy and data protection Commissioners appealed 'to the Council of Europe to invite, in accordance with article 23 of the Convention … non-member-states of the Council of Europe which already have a [sic] data protection legislation to accede to this Convention and its additional Protocol.' It is worth noting that the EU – or, more accurately, European Communities (EC) – has long signaled a wish to accede to the Convention. Amendments to the Convention were adopted in 1999 in order to permit accession by the EC but are not yet in force.[9]

Since 2001, a similar approach has seen the Council of Europe *Cybercrime Convention* become an international instrument of widespread adoption outside Europe. It is a way of sidestepping the cumbersome process of developing a new UN convention on privacy, by starting with an instrument already adopted by the region with the most concentrated distribution of privacy laws. This approach deserves serious consideration by Australia, New Zealand, Japan, South Korea and other Asia-Pacific countries with privacy legislation approximating OECD and Council of Europe standards, as it could provide a reasonable basis (a common reasonably high privacy standard) for a guarantee of free flow of personal information between parties to the treaty, both as between Asia-Pacific countries and as between those countries and European countries. As other countries outside Europe or the Asia-Pacific adopt serious privacy legislation, as South Africa soon may, joint membership of this Convention would also guarantee data transfers between these countries and Australia. Such invitation and accession would also be likely to carry with it the benefits of a finding of 'adequacy' under the EU Directive, given that the 2001 Additional Protocol (Council of Europe 2001) to the Convention has added a data export restriction and a requirement of an independent data protection authority to bring it more into line with the EU privacy Directive.

Given that the APEC Privacy Framework has not attempted to provide such a general legislation-based mechanism for free flow of personal information within the Asia-Pacific, perhaps globalizing this European instrument is now the realistic way open to do so. It would also be a much quicker solution than waiting for some new global enforceable treaty to emerge from the UN or elsewhere.

> ***Submission DP72-116: The ALRC should recommend to the Australian Government that it seek to accede to the Council of Europe's privacy Convention No 108, as this would: (i) guarantee free flow of personal information between Australia and Europe; (ii) be likely to assist similarly***

[9] See Amendments to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) allowing the European Communities to accede. The amendments will enter into force on the thirtieth day after approval by all of the Convention Parties (Art. 21(6) of the Convention). As of 1.12.2006, 26 Parties had registered their approval.

in relation to some non-European countries over time; and (iii) demonstrate the strength of Australia's privacy laws internationally.

Trustmarks

Question 28–2: Would the use of trustmarks be an effective method of promoting compliance with, and enforcement of, the Privacy Act and other international privacy regimes? If so, should they be provided for under the Privacy Act?

There is no evidence that trustmarks have anything of value to contribute to privacy protection. If the whole of the Australian private sector will now be required to comply with high standard privacy laws, it is hard to see that there is a lot of point in trustmarks. In most cases it would just constitute Australian businesses pretending to have some pseudo-accreditation that adds little if anything to their legal obligations. There may however be some exception for online businesses, who operate in an international context where their compliance with Australian and other national laws (and perhaps some other standards) may provide some genuine mark of differentiation from their competitors. In such cases their might be some justification for OPC involvement in a trustmark scheme, provided it also involved consumer organisations in its operation. Public resources should not be lightly spent on anything to do with trustmarks in Australia, but there may be unusual cases where it can be shown that they add something of value, as well as situations where they constitute false and misleading conduct.

Submission DP72-117: Trustmarks should not be provided for in the Privacy Act, and OPC should not be involved with them except where there is a compelling case of value to consumers, and the involvement of consumer organisations in their operation.

Privacy Commissioner's roles

The ALRC proposes that the Office of the Privacy Commissioner should develop and publish guidance on the proposed UPP 11, including guidance on: (a) when personal information may become available to a foreign government; (b) outsourcing government services to organisations outside Australia; (c) the issues that should be addressed as part of a contractual agreement with the overseas recipient of personal information; (d) when a transfer of personal information is 'for the benefit' or 'in the interests of' the individual concerned; (e) what constitute 'reasonable steps' to ensure the information it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the proposed UPPs (DP72, Proposal 28-9), and on what constitutes a 'reasonable belief' (DP72, [28.50]). We refer to our generic concerns about OPC guidance in our submission on Part F of DP72.

Submission DP72-118: The OPC should be required by the Act to publish guidelines as proposed in Proposal 28-9.

We support the ALRC's encouragement to the Australian Government and the OPC to continue to seek opportunities for further cooperation with privacy regulators outside Australia (DP72, [24.104]).

14.6. Extra-territorial operation of the *Privacy Act*

We support the ALRC's proposal to amend the *Privacy Act* to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency and not only by an organisation (DP72, Proposal 28-1).

14.7. Related bodies corporate

We support the ALRC's proposal to amend section 13B of the *Privacy Act* to clarify that, if an organisation transfers personal information to a related body corporate outside Australia, this transfer will be subject to the proposed UPP 11 (DP72, Proposal 28-7).

15. Additional Privacy Principles

15.1. Possible new UPP - Security breach notification

We support the general thrust of the ALRC's proposals concerning data breach notification (DP72, Chapter 47 and Proposal 47-1), but are dealing with the matter here because we consider that this should either be an additional UPP 12, or alternatively part of UPP 8 (Security), since it is the consequence of a security breach (UPP 8(2)?). Any mechanical aspects could go elsewhere in the Act, but the basic 'high level' principle should in our view be found in the UPPs. This would make it more likely that data breach notification will be adopted in Australian state and Territory public sectors' privacy law, than if the provisions are only in procedural or enforcement parts of the Act, which will tend to vary more between jurisdictions.

> ***Submission DP72-119: The general principle of requiring data security breaches to be notified under certain circumstances should be included in the UPPs, either as a new UPP or (preferably) as part of the security principle.***

ALRC proposal for data breach notification

> *Proposal 47–1 The Privacy Act should be amended to include a new Part on data breach notification, to provide as follows:*
>
> *(a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.*
>
> *(b) An agency or organisation is not required to notify any affected individual where:*
>
> *(i) the specified information was encrypted adequately;*
>
> *(ii) the specified information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the proposed Unified Privacy Principles (provided that the personal information is not used or subject to further unauthorised disclosure); or*
>
> *(iii) the Privacy Commissioner does not consider that notification would be in the public interest.*
>
> *(c) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.*

Improvements recommended to data breach notification

We suggest that the ALRC's approach could be improved in the following ways.

If 'the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual' (as in (a) above) then there is no reason to limit the requirement to notify to specified classes of information – the likelihood of serious harm is enough of trigger in itself. Consistent with its approach elsewhere, the ALRC would do better to require the OPC to issue guidelines on what types of information are most likely to require such notification.

> ***Submission DP72-120: In ALRC Proposal 47–1 (a) the word 'specified' should be deleted. The OPC should be required to issue guidelines on when such notifications are likely to need to be given.***

It would also be better if it was more clear that (b) provided exceptions to (a), and that an organisation/agency may first notify the Privacy Commissioner before notifying individuals. Provision (b)(iii) also needs to specify that the Commissioner may defer a requirement to notify individuals while the Commissioner considers whether to exercise his powers under (iii). We submit that OPC should not have what would be in effect an uncheckable discretion to decide it is 'better that we don't know'. OPC's discretion under (b)(iii) should be limited to (a) substituting its view for that of the agency/organisation to the effect that 'there is no real risk of serious harm to any affected individual', or (b) deferring any requirement of notification (on public interest grounds) for a specified period, so that (for example) police investigations can take place. OPC should have to report to Parliament on exercise of this power.

> ***Submission DP72-121: In ALRC Proposal 47–1 (b), the OPC's powers should be limited to (a) substituting its view for that of the agency/organisation to the effect that 'there is no real risk of serious harm to any affected individual', or (b) deferring any requirement of notification (on public interest grounds) for a specified period. An organisation/agency should be allowed to first notify the Privacy Commissioner before notifying individuals. OPC should be able to defer an organisation's obligation to disclose for a specified time while OPC decides whether it will act under (b).***

Provision (c) needs to be amended, if this becomes part of a Principle, to clarify that any civil penalty is additional to the usual remedies for breach of a Principle. There are broader public interests in maintaining security standards here irrespective of harm to any one individual, that justify such additional penalties.

> ***Submission DP72-122: In ALRC Proposal 47–1(c), any civil penalties should be additional to normal remedies for breach of a UPP.***

15.2. Accountability Principle

We support the ALRC's view that the proposed UPPs should not contain a discrete accountability principle (see CLPC IP 31, p. 54; DP72, [29.13)]. The existing models seem to add little substance. The OECD accountability principle (14) is nothing more than a 'motherhood' statement, while the APEC Framework Accountability principle (IX) seems to be more to do with onward transfer obligations that are arguably best covered in security and transborder data principles, and also seems confused about the

role of consent. We agree with the ALRC that there are better mechanisms for establishing accountability and that an accountability principle may be of limited practical utility (DP72, [29.13]-[29.14]).

15.3. Prevention of Harm Principle

We support the ALRC's view that the UPPs should not contain a discrete 'prevention of harm' principle (CLPC IP 31, Submission 4-35; DP72, [29.22]). A separate principle of 'preventing harm' which is found in the APEC Framework (Principle I) is not much more than re-statement of the overall objective of information privacy laws and so we support the ALRC's suggestion that a number of the principles in the UPPs already incorporate a prevention of harm approach (DP72, [29.23]) and concur with concerns that the obligations of a general prevention of harm principle will be undesirably vague (DP72, [29.24]).

15.4. No Disadvantage Principle

The ALRC supports the general objective of a 'no disadvantage' principle, but does not believe that a separate principle in the UPPs is the most appropriate vehicle to achieve this. The ALRC's view is that this requirement should be incorporated, where appropriate, into some of the other privacy principles and in guidance from the OPC. (DP72, [29.33]) We doubt that such measures can adequately substitute for a principle such as 'People should not be denied goods or services or offered them on unreasonably disadvantageous terms (including higher cost) in order to enjoy the rights described in this Charter' (as in the Australian Privacy Charter and the Asia Pacific Privacy Charter).

We adhere to our previously expressed view (CLPC IP31, Submission 4-35.3) that without a broader 'no disadvantage' principle, it is all too easy for data users to levy a charge for the exercise of privacy choices and rights, either directly, or by differential pricing, or to impose some other non-financial barrier. We recognise that it can be difficult to distinguish actions deliberately designed to deter the exercise of privacy rights from the incidental effect of new services or technologies, and for this reason suggest a modified version.

> ***Submission DP72-123: Privacy law should include an additional no-disadvantage principle to ensure that data users do not use pricing or other sanctions that deter individuals from exercising their privacy rights, to the extent that this is practicable.***

If this is not accepted, we agree with the ALRC that one useful way in which the 'no disadvantage' objective can be incorporated into the operation of the privacy principles more generally is through careful interpretation of the requirement on agencies and organisations to take 'reasonable steps' to protect individuals' information privacy in particular respects. (DP72, [29.35]). We also agree that, if an individual requests access to an agency's or organisation's Privacy Policy, the proposed 'Openness' principle provides that the agency or organisation must take reasonable steps to make this available without charging the individual for it (DP72, [29.33]).

There are other Principles where consideration should be given to ensuring that individuals are not disadvantaged in exercising their privacy rights, including: (i) the

Anonymity Principle, where it is very easy for organisations to make it very burdensome for individuals to exercise anonymity or pseudonymity options; (ii) the Security Principle, where charges should only be allowed for security measures that go beyond what can reasonably be required to protect a person's privacy.

15.5. Consent or 'choice' principle

In our earlier submission we made a case for a consent or 'choice' principle (CLPC IP31, Submission 4-35.1). The ALRC does not expressly address this suggestion in DP 72.

We now consider that issues of choice and consent can be addressed adequately in other principles, and no longer suggest an additional principle.

15.6. Automated decision-making principles

In our earlier submission we made a case for an 'automated decision-making' principle (CLPC IP 31, Submission 4-35.4). The ALRC addresses this issue in its consideration of accommodating developing technology (DP72, Chapter 7). The ALRC notes the 2004 report of the Administrative Review Council on Automated Assistance in Administrative Decision Making, and supports the practice of human review of decisions that are made by automated means, particularly when an agency or organisation plans to take adverse action against an individual on the basis of such a decision (DP72, [7.106]). However, the ALRC concludes that this should only be the subject of guidance issued by the OPC (DP72, [7.107]).

We agree with the ALRC that the proposed 'Data Quality' principle (though not the 'Access and Correction' principle) in the UPPs could be taken to impose such a requirement in some circumstances, but submit that it should be made an express requirement as part of UPP 7, with an appropriate 'reasonable steps' limitation.

> ***Submission DP72-124: The Data Quality principle (UPP 8) should provide that an organisation or agency should take reasonable steps to avoid making a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human.***

15.7. Privacy impact assessments principles

In our earlier submission we proposed a principle requiring privacy impact assessment (PIA) in appropriate circumstances (CLPC IP31, Submission 4-35.5). The ALRC has addressed the issue of privacy impact assessment in the part of the Discussion Paper dealing with enforcement and the role of the Privacy Commissioner (DP72, Part F – Chapter 44) and makes proposals in relation to requirements for PIA, (DP72, Proposals 44-4 and 44-5). We comment in our separate submission on those proposals.

References

Australian Law Reform Commission ('DP72'),, Discussion Paper 72: Review of Australian Privacy Law, September 2007.

APEC Framework Part B - *APEC Privacy Framework International Implementation ("Part B") Final* – Version VII ECSG Plenary Meeting Gyeongju, Korea, 8-9 September 2005.

Bygrave, L. 2002, *Data Protection Law: Approaching Its Rationale, Logic and Limits* Kluwer Law International, 2002).

Council of Europe 1981, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* (Convention No 108).

Council of Europe 2001, *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, Strasbourg, 8.XI.2001.

Data Protection Working Party 2007, *Opinion 4/2007 on the concept of personal data*, at < http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf>

Greenleaf, G., Waters, N, and Bygrave L ('CLPC IP31'). 'Implementing privacy principles: After 20 years, its time to enforce the *Privacy Act*', Submission to the Australian Law Reform Commission on the Review of Privacy Issues Paper, January 2007,

Greenleaf G 'Key concepts undermining the NPPs - A second opinion' (2001) 8 *Privacy Law & Policy Reporter* 1

Gunning, P. 2001, 'Central Features of Australia's Private Sector Privacy Law' 7(10) *Privacy Law and Policy Reporter* 189

Montreux Declaration 2005, 'The protection of personal data and privacy in a globalised world: a universal right respecting diversities', Declaration of the 27th International Conference of privacy and Data Protection Commissioners, Montreux, Switzerland, September 2005.

OECD 1981, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Paris: OECD, 1981).

Office of the Privacy Commissioner ('OPC') March 2005, *Getting in on the Act: Review of the Private Sector provisions of the Privacy Act 1988.*

Index of Submissions

1. Key Terminology

Submission DP72-1: The definition of 'personal information', or the explanatory memorandum in relation thereto, should state that it covers those situations where information is sufficient to allow interaction with persons on an individualised basis, or the imparting of consequences on an individualised basis. This should not include information which merely allows an individual to be contacted without conveying anything about the individual's identity or characteristics.

Submission DP72-2: The ALRC should re-visit the question of genetic samples in the context of this review.

Submission DP72-3: We support Proposal 3–8 but submit that if it is adopted, there will need to be a corresponding clarification that 'a person' is not an 'other form' of storage.

2. Structural Reform of the Privacy Principles

Submission DP72-4: The proposed new set of privacy principles should be known as the Uniform Privacy Principles

3. Consent

Submission DP72-5:The definition of 'consent' should be amended to deal with a number of key issues concerning consent, specified in the following submissions, rather than leaving them to OPC guidance. Other aspects of consent should be dealt with where possible in the Explanatory Memorandum, and only otherwise by OPC guidance.

Submission DP72-6: Whether or not our submission DP72-5 is accepted, we submit that the OPC should be required to issue guidelines on a specified list of issues concerning consent within one year.

Submission DP72-7: In relation to implied consent, either the definition of 'consent' or the explanatory memorandum should state that implied consent must be clear and not ambiguous.

Submission DP72-8: Either the Act or the Explanatory Memorandum should state that a failure to opt out is not by itself to constitute consent.

Submission DP72-9: The ALRC should give further consideration to the implications of the confusion caused by the lack of any distinction in the Privacy Act between uses or disclosures justified by consent and those justified by acknowledgment of notification. At the least, the Act or the Explanatory Memorandum should state that where a person has no choice but to provide personal information in order to obtain a benefit, no consent to any uses of the information beyond the express purpose of collection may be implied. In such circumstances of 'involuntary consent', only express consent should apply.

Submission DP72-10: The definition of 'consent' needs to be amended in order to prevent abuse of the practice of 'bundled consent'. In particular, wherever consent is applicable to the operation of a privacy principle, separate consent should be required for each proposed purpose of use.

4. Anonymity and Pseudonymity (UPP 1)

Submission DP72-11: UPP 1 should state that 'agencies and organisations must give individuals the option of anonymity/pseudonymity, not that 'individuals … should have' this option. (This reformulation is also necessary in relation to our next submission).

Submission DP72-12: UPP 1 should expressly state that the obligation on organisations/agencies applies at the stage when an information system is being designed, not only 'after the event' when a person wishes to enter a transaction with a data user. This is to mean that where it is practicable, without excessive cost, to design anonymity/pseudonymity options into a system, they must be designed in. The judgements as to practicability and as to whether any cost is excessive must not be left to the organisation/agency – they must be able to be tested by an independent party.

Submission DP72-13: The anonymity principle should impose an obligation on organisations to facilitate, where practicable and lawful, anonymous or pseudonymous transactions between individuals and third parties

Submission DP72-14: The words '..,provided this is not misleading' should be deleted from paragraph (b) of UPP1.

Submission DP72-15: UPP 1 should read: "An agency or organisation must, where lawful and practicable, give individuals the option of either:

(a) not identifying themselves; or

(b) identifying themselves with a pseudonym

This obligation applies both in the operation of an information system and at the stage when a system is being designed, and should include facilitation of anonymous or pseudonymous transactions between individuals and any third parties for whose use the system is designed."

5. Collection (UPP 2)

Submission DP72-16: The Act or Explanatory Memorandum should make it clear that unsolicited information is included within the meaning of 'collect'.We comment further below on other means of collection.

Submission DP72-17: Add to UPP 2.1 the words '…and is proportional to those functions or activities'.

Submission DP72-18: Add to UPP 2.1 a second sentence: 'The perceived necessity must be related to the particular purpose of collection of the information in question.'.

Submission DP72-19: UPP 2.1 should refer to 'one or more of its lawful functions or activities.'. .

Submission DP72-20: The consent exception in UPP 2.6(a) should require express or explicit consent.

Submission DP72-21: The exception (b) in UPP 2.6 should include the word 'specifically'.

Submission DP72-22: We oppose the deletion of the word 'imminent' from UPP 2.6(c)

Submission DP72-23: The first paragraph of UPP 2.6(d) should read 'if the information is collected in the course of the lawful activities of a non-profit organisation that has aims relating to sensitive information (as defined in this Act) – the following conditions are satisfied:'

Submission DP72-24: The Privacy Commissioner should be required to issue guidance about fair and lawful means of collection, which are of considerable practical importance.

Submission DP72-25: UPP 2.4 should be deleted

Submission DP72-26: The law should make it clear that the collection principles UPPs 1 and 2 apply to the maximum practical extent to information obtained from observation or surveillance; to information extracted from other records, and to information generated within and organisation/agency as a result of transactions. This should be done either in the legislation or in the Explanatory Memorandum.

Submission DP72-27: Different notification requirements may appropriately be modified depending on how the data is collected, with the default position being that notice is required unless an exception is provided in UPP 3. The Privacy Commissioner should be required to issue guidance about compliance with the specific notification requirements under UPP 3 in relation to different circumstances of collection.

Submission DP72-28: The ALRC should address the issue of how Australian law should clarify the relationships between collection and disclosure of personal information, and in particular the limitations that the purposes of collection of a first organisation play in limiting the uses of a second organisation to which the information is disclosed. If this is not done in the legislation, it would nevertheless be valuable to have the Explanatory Memorandum clarify what is the expected interpretation of the legislation.

Submission DP72-29: The ALRC should address the issue of the role that the law of breach of confidence plays in determining the circumstances under which the use or disclosure of personal is limited. In particular the principles in Johns v ASC and similar cases, insofar as they apply to personal information, should be supported by statutory provisions in the Privacy Act.

6. Specific Notification (UPP 3)

Submission DP72-30: To ensure that all circumstance of collection are covered, the words 'by any means' should be inserted in UPP 3 as follows: '…..from the individual, by whatever means, it must take …'

Submission DP72-31: UPP 3.1 should be re-worded from '… reasonable steps to ensure that the individual is aware' to '…reasonable steps to notify the individual or otherwise ensure that the individual is aware' .

Submission DP72-32: UPP 3.3 should be re-worded as follows:

'An agency or organisation must comply with the obligations in UPPs 3.1 and 3.2 unless:

(a) it reasonably believes that the individuals concerned do not expect to be notified

Submission DP72-33: UPP 3.3(b)(i) should only apply to indirect collection. As such, it may be better relocated to UPP 3.2.

Submission DP72-34: Exception (b)(ii) in UPP 3.3 should apply both to agencies and to organisations.

Submission DP72-35: The explanation '(for example, how, when and from where the information was collected)' should be deleted from UPP 3.1(a) and given instead in a Note or further guidance.

Submission DP72-36: UPP 3.1(b) should include the word 'functional' before 'contact details'.

Submission DP72-37: UPP 3.1(c) should read 'fact that the individual is able to gain access to the information and seek correction;'

Submission DP72-38: We support the inclusion of items (d) and (e) in UPP 3.1

Submission DP72-39: We support the inclusion of information about usual disclosures as UPP 3.1(f).

Submission DP72-40: We support the inclusion of item (g) in UPP 3.1.

Submission DP72-41: Proposed UPP 3.2(b) should be amended to read: 'the identity of the source of the information, if requested by the individual.'

Submission DP72-42: Proposed UPP 3.2 should be amended at the end of the first paragraph to read '… the individual is or has been made aware, at or before the time of that collection (or, if that is not practicable, as soon as practicable thereafter) of:'

7. Openness (UPP 4)

Submission DP72-43: We support Proposal 21-1 for a discrete Openness principle to apply both to agencies and to organisations.

Submission DP72-44: We support Proposal 21-2 for the proposed content of UPP 4.1.

Submission DP72-45: We support Proposal 21-4 for the wording of UPP 4.2.

Submission DP72-46: UPP 4 should include a requirement: 'an agency must submit an electronic copy of its privacy policy to the Privacy Commissioner at least once each year'.

Submission DP72-47: Any privacy policies submitted to the Privacy Commissioner should be published by the Privacy Commissioner, and may be republished by other parties'.

Submission DP72-48: The Privacy Commissioner, by legislative instrument, should be able to require a class of organisations to submit an electronic copy of their privacy policies to the Privacy Commissioner at least once each year.

Submission DP72-49: Regulations or a binding Code should prescribe the minimum set of information which needs to be provided at or before the time of collection to achieve the objective of the specific notification principle (UPP 3) and the minimum standard of transparency of links to more detailed information provided under UPP 4.

8. Use and Disclosure (UPP 5)

Submission DP72-50: On balance, we support Proposal 22-1 for a single 'use and disclosure' principle.

Submission DP72-51: Either this principle, the definitions, or the Explanatory Memorandum, should confirm that accessing personal information, even without further action being taken as a result of that access, is 'use' of personal information.

Submission DP72-52: Either this principle, the definitions, or the Explanatory Memorandum, should clarify the circumstances in which passing information outside an organisation remains a use rather than a disclosure

Submission DP72-53: Either this principle, the definitions, or the Explanatory Memorandum, should make it clear that there can be a disclosure even if the information is not used or acted on by the third party, and that even information already known to the recipient it can still be 'disclosed'.

Submission DP72-54: The law should be clarified to expressly allow for the declaration of multiple specific purposes, but not to allow a broadly stated purpose .

Submission DP72-55: We support the proposed exception UPP 5.1 (a).

Submission DP72-56: We support the proposed exception UPP 5.1 (b).

Submission DP72-57: We oppose the deletion of the qualifying word 'imminent' from UPP 5.1(c)

Submission DP72-58: We support the proposed exception UPP 5.1 (d).

Submission DP72-59: We support a narrowing of the proposed exception UPP 5.1 (e) to include 'specifically'.

Submission DP72-60: We support the proposed exception UPP 5.1 (f). We suggest that there should be a Note to this exception stating that it requires the active involvement of an Australian enforcement body

Submission DP72-61: UPP 5 should include a specific requirement to keep a log or record of all uses and disclosures for secondary purposes under exceptions (a)-(f).

Submission DP72-62: There should be a clear statement, either by note in the Act (the preferred option) or in the Explanatory Memorandum in relation to UPP 5 that all the exceptions apart from (e) are discretionary and are neither a requirement nor an authorisation to use or disclose.

9. Direct Marketing (UPP 6)

Submission DP72-63: The Privacy Act should define 'direct marketing' as 'the marketing or promotion of goods, services or ideas, including fundraising and recruitment, by direct targeted communication with specific individuals or by individualised communications, by any means.'

Submission DP72-64: We support Proposal 23-1 for a separate Direct Marketing principle.

Submission DP72-65: UPP 6 should apply both to agencies and to organisations.

Submission DP72-66: UPP 6 should contain another exception as an alternative to conditions (b)-(e) so that 6.1 would read: '… unless the following conditions are met:

(a) [as proposed by the ALRC]

and either

(b) the use of information for direct marketing is required or specifically authorised by or under law,

or

(c) all of the following conditions are met:

[(b)- (e) in current proposal renumbered as sub-items within (c)]

Submission DP72-67: Any sectoral legislation addressing direct marketing should as far as possible be consistent with UPP 6. Any weakening of the standards in UPP 6 should be clearly justified and should be included in the Privacy Act as exceptions to UPP 6.

Submission DP72-68: UPP 6.1(e) should be amended to read '….each communication by the [organisation] with the individual includes a functional means of contacting the [organisation]. If the communication is by electronic means, the means of contact must be at least as easy to use.

Submission DP72-69: UPP 6.1(c) should be amended to read 'the individual has not made a request, either directly or indirectly, to the [agency or] organisation …'.

Submission DP72-70: Either Regulations or a binding Code should prescribe specific response times for different media of communication, to give effect to individuals' requests not to receive further direct marketing communications.

Submission DP72-71: UPP 6.3 should be amended to read '…to advise the individual of the identity of the source of the individual's personal information.'

Submission DP72-72: The Privacy Commissioner should be required to issue guidance about compliance with UPP 6, including specifically the matters specified in proposal 23-6, and the practicalities of compliance when using different communications media.

10. Data Quality (UPP 7)

Submission DP72-73: There should be a clear statement, either by note in the Act (the preferred option) or in the Explanatory Memorandum that in assessing what steps are reasonable under UPP 7, primary regard shall be given to the extent to which data-processing error can have detrimental consequences in the context of the particular information and circumstances.

Submission DP72-74: UPP 8.2 should state 'An agency or organisation must take reasonable steps to ensure that the personal information it uses or discloses for a purpose other than the purpose of collection is accurate, complete, up-to-date and relevant in relation to that purpose, unless it is required by law to disclose the information.'

11. Data Security (UPP 8)

Submission DP72-75: UPP8 should be re-worded to require protection against 'improper access, use, alteration, deletion or disclosure, or other misuse, by both authorised users and by other parties'.

Submission DP72-76: UPP 8 should also state that 'For the purposes of this Principle, reasonable steps must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information.'

Submission DP72-77: OPC should be required by the Act to issue guidelines on the meaning of 'reasonable steps' within one year.

Submission DP72-78: UPP 8(b) should be a separate Data Retention principle

Submission DP72-79: The Act should define 'render non-identifiable' as 'taking reasonable steps to prevent future re-identification of personal information'.

Submission DP72-80: The data retention principle (whether part of UPP 8 or separate) should provide that personal information must only be retained for any secondary purpose for which it has already legitimately been used, or for which there is express legal authority for retention. A Note should explain that secondary purposes for which personal information may be used or disclosed in future do not provide an alternative justification for retention

Submission DP72-81: The OPC should be required by the Act to issue guidelines on the retention principle within one year.

Submission DP72-82: ALRC should give further consideration as to whether there are any circumstances where a person should be able to put forward a case for destruction rather than non-identifiability of their data.

Submission DP72-83: The obligation in UPP 8(c) should apply to all 'personal information it discloses to a third person'.

Submission DP72-84: The obligation in UPP 8(c) should extend to requiring third party recipients of personal information to observe all relevant UPPs in relation to that information.

12. Access and Correction (UPP 9)

Submission DP72-85: We support the inclusion in the UPPs of an access and correction principle (UPP 9) applying only to organisations.

Submission DP72-86: UPP 6.1(e) should be amended to add a second sentence: 'The extent of the refusal must be proportionate to the significance of the negotiations'.

Submission DP72-87: UPP 6.1(g) should be amended to insert 'specifically' before 'authorised'.

Submission DP72-88: A Note should be added after UPP 6.1 to remind organisations that exception (i) requires the active involvement of an Australian enforcement body.

Submission DP72-89: The Note after UPP 9.2 should be replaced by one advising that 'The mere fact that some explanation may be necessary in order to understand information such as a score or algorithm result should not be taken as grounds for withholding information under 9.2.'.

Submission DP72-90: UPP 9.3 should be amended to replace 'provided that would allow for sufficient access to meet the needs of both parties' with 'to allow for access to at least some of the information.'

Submission DP72-91: UPP 9.3 should be amended to add 'In the absence of agreement, the Privacy Commissioner would be the intermediary.' The Privacy Commissioner should be empowered to act as an intermediary in the context of UPP 9.3.

Submission DP72-92: The Office of the Privacy Commissioner should be expressly required to issue guidance to the effect that organisations should only claim any relevant exceptions (grounds for withholding) to the minimum extent necessary and that they should wherever possible provide as much of the information held as possible, even if this means selective editing or suppression of material subject to one of the exceptions.

Submission DP72-93: Either Regulations or a binding Code should set benchmarks for response times and fees in relation to access and correction requests.

Submission DP72-94: UPP 9.5 should be amended to read 'to establish on the balance of probabilities …'

Submission DP72-95: UPP 9.5 should be amended to read 'with reference to the purpose(s) for which the information was collected.'

Submission DP72-96: The Privacy Commissioner should be required to issue guidance to the effect that correction can take the form of amendment, deletion or addition, as appropriate in the circumstances. The guidance should also advise that there are many situations where there is a legal requirement to keep an historical record of actual transactions, but that this should not prevent the correction of 'operational' records, leaving the original incorrect information only in an archive.

Submission DP72-97: Where an agency or organisation makes a correction to personal information about a person which has previously been used or disclosed under circumstances which is reasonably likely to have had an adverse effect on the person, they should inform the person of the correction and of any such previous disclosures of the information. e. Such an obligation could be located in UPP 7, UPP 9 or integrated with the proposed new data breach notification obligation wherever that is located.

Submission DP72-98: UPP 9.6 should specify that the obligation in relation to disputed information has to be performed in a way which ensures that any annotation is made available to any subsequent user of the disputed information.

Submission DP72-99: UPP 9.7 should be amended to add a second sentence: 'The reasons should specify which of the exceptions in UPP 9 apply.' The OPC should issue guidance on the application of this sub-principle.

13. Identifiers (UPP 10)

Submission DP72-100: The definition of 'identifier' should also encompass when identifiers are used for authentication (verification) and not only when used for identification.

Submission DP72-101: UPP 10.3 and UPP 10.4(d) should be deleted, and any exceptions left to the public interest determination process.

Submission DP72-102: We support the application of UPP 10 to identifiers that are assigned by state and territory agencies

Submission DP72-103: The Act should require that, before the introduction by agencies of any unique multi-purpose identifier, an independent and public privacy impact assessment should be commissioned, the terms of reference of which should be a determination by the Privacy Commissioner, such a determination being a legislative instrument. Any exceptions to UPP10 should be clearly set out in legislation.

Submission DP72-104: OPC should be required by the Act to review within one year the Tax file number (TFN) Guidelines (Rules) so as to make them consistent with UPP 10.

14. Transborder Data Flows (UPP 11)

Submission DP72-105: 'Transfer' should include where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia. However, the ALRC should consider whether as a result any additional exception allowing some transfers in non-business and non-government settings should be made.

Submission DP72-106: A 'transfer' should only occur if there is a recipient outside Australia who uses or stores the information for purposes other than communicating it to its final recipient. Communications may involve temporary storage, but if the information is subject to set retention periods whether required by law or otherwise, there will be a transfer.

Submission DP72-107: Any 'whitelist' in relation to UPP 11(a) should be by a regulation or other legislative instrument made by the government, and made after receipt of published advice from the Privacy Commissioner.

Submission DP72-108: In order to qualify for the 'whitelist' for the purposes of UPP 11(a), a foreign jurisdiction must have in place an agreement on cross border enforcement with the Australian Privacy Commissioner.

Submission DP72-109: Except where a transfer is to a jurisdiction included in a 'whitelist' legislative instrument, the agency or organisation should continue to be liable for any breaches of the UPPs (as in exception (d)).

Submission DP72-110: UPP condition (b) should require that the individual 'expressly' consents to the transfer.

Submission DP72-111: UPP 3 should provide for the individual concerned to be given notice of the specific country or countries to which the data may be transferred. The consent exception (b) in UPP 11 should be conditional on (i) compliance with this aspect of UPP 3, and (ii) notice when obtaining express consent of the fact that the transferor will no longer be liable for any breaches. The consent exception should also be conditional upon the obligation in UPP 11 (d)(v).

Submission DP72-112: Any 'enforcement' exception to UPP11 must be more tightly worded and conditional.

Submission DP72-113: In UPP 11, condition (d)(v) should apply to all transfers on the basis of (d)(i)-(iv), as well as to transfers on the basis of consent (exception (b)), and by or on behalf of enforcement bodies (exception (c)).

Submission DP72-114: There should be a requirement to inform individuals that their personal information is to be transferred to any jurisdiction without equivalent privacy protection (including some State jurisdictions within Australia). If the organisation has an intention to transfer at the time of collection, it should give notice at that point. If it later decides to export the data, it should give notice at that time.

Submission DP72-115: There should also be a requirement to inform individuals of the jurisdiction(s) to which their personal information is to be transferred, and the identity of the recipient(s) in the(se) jurisdiction(s).

Submission DP72-116: The ALRC should recommend to the Australian Government that it seek to accede to the Council of Europe's privacy Convention No 108, as this would: (i) guarantee free flow of personal information between Australia and Europe; (ii) be likely to assist similarly in relation to some non-European countries over time; and (iii) demonstrate the strength of Australia's privacy laws internationally.

Submission DP72-117: Trustmarks should not be provided for in the Privacy Act, and OPC should not be involved with them except where there is a compelling case of value to consumers, and the involvement of consumer organisations in their operation.

Submission DP72-118: The OPC should be required by the Act to publish guidelines as proposed in Proposal 28-9.

15. Additional Privacy Principles

Submission DP72-119: The general principle of requiring data security breaches to be notified under certain circumstances should be included in the UPPs, either as a new UPP or (preferably) as part of the security principle.

Submission DP72-120: In ALRC Proposal 47–1 (a) the word 'specified' should be deleted. The OPC should be required to issue guidelines on when such notifications are likely to need to be given.

Submission DP72-121: In ALRC Proposal 47–1 (b), the OPC's powers should be limited to (a) substituting its view for that of the agency/organisation to the effect that 'there is no real risk of serious harm to any affected individual', or (b) deferring any requirement of notification (on public interest grounds) for a specified period. An organisation/agency should be allowed to first notify the Privacy Commissioner before notifying individuals. OPC should be able to defer an organisation's obligation to disclose for a specified time while OPC decides whether it will act under (b).

Submission DP72-122: In ALRC Proposal 47–1(c), any civil penalties should be additional to normal remedies for breach of a UPP.

Submission DP72-123: Privacy law should include an additional no-disadvantage principle to ensure that data users do not use pricing or other sanctions that deter individuals from exercising their privacy rights, to the extent that this is practicable.

Submission DP72-124: The Data Quality principle (UPP 8) should provide that an organisation or agency should take reasonable steps to avoid making a decision adverse to the interests of an individual based on automated processing, without the prior review of that decision by a human.