Unified Privacy Principles – the right way ahead: comments to the Federal Department of Prime Minister and Cabinet on the draft UPPs

2 February 2009

Robin Banks, Chief Executive Officer

Level 9, 299 Elizabeth Street, Sydney NSW 2000 • DX 643 Sydney
Phone: 61 2 8898 6500 • Fax: 61 2 8898 6555 • www.piac.asn.au

Contents

Introduction

The Public Interest Advocacy Centre

The Public Interest Advocacy Centre (PIAC) is an independent, non-profit law and policy organisation that works for a fair, just and democratic society, empowering citizens, consumers and communities by taking strategic action on public interest issues.

PIAC identifies public interest issues and, where possible and appropriate, works co-operatively with other organisations to advocate for individuals and groups affected. PIAC seeks to:

- expose and redress unjust or unsafe practices, deficient laws or policies;
- promote accountable, transparent and responsive government;
- encourage, influence and inform public debate on issues affecting legal and democratic rights;
- promote the development of law that reflects the public interest;
- develop and assist community organisations with a public interest focus to pursue the interests of the communities they represent;
- develop models to respond to unmet legal need; and
- maintain an effective and sustainable organisation.

Established in July 1982 as an initiative of the Law Foundation of New South Wales, with support from the NSW Legal Aid Commission, PIAC was the first, and remains the only broadly based public interest legal centre in Australia. Financial support for PIAC comes primarily from the NSW Public Purpose Fund and the Commonwealth and State Community Legal Services Program. PIAC also receives funding from the NSW Government Department of Water and Energy for its work on utilities, and from Allens Arthur Robinson for its Indigenous Justice Program. PIAC also generates income from project and case grants, seminars, consultancy fees, donations and recovery of costs in legal actions.

PIAC's work on privacy

PIAC has a long history of interest in, and concern about, the appropriate protection of privacy rights within both the public and private sectors. PIAC has been a strong advocate for the protection of the privacy rights of Australians, particularly the rights of individual Australians to control their personal information and to be free of excessive intrusions. PIAC's work as a consumer advocacy organisation, particularly in relation to health matters, has required PIAC to consider privacy issues because they are frequently a matter of concern to many people who contact the Centre.

In recent years, PIAC has provided legal advice and assistance to clients in a number of matters involving alleged breaches of the *Privacy and Personal Information Protection Act 1998* (NSW) (the PPIP Act) and the *Privacy Act 1988* (Cth) (the Privacy Act). In 2006, PIAC represented the respondent in *Director General, NSW Department of Education and Training v MT* [2006] NSWCA 270, a landmark case concerning the interpretation of several provisions of the PPIP Act. In another matter, currently before the Office of the Privacy Commissioner (OPC) PIAC is representing a former Villawood detainee whose personal information was allegedly inappropriately disclosed to the media.

PIAC has played a leading role in privacy debates in Australia in recent years, contributing to a number of inquiries and reviews at the national and state level. Recent submissions by PIAC have addressed the

privacy implications of the proposed Health and Social Services Access Card[1], and the proposal by the Australian Bureau of Statistics to implement a longitudinal study in the population census (a proposal requiring capacity to data match over time).[2] In October 2007, PIAC made a submission to the first Consultation Paper in the current reference from the New South Wales Law Reform Commission (NSW LRC), *Consultation Paper 1 – Invasion of Privacy*.[3] In December 2007, PIAC made a submission in response to *DP72: Review of Australian Privacy Law* (DP 72)[4], as part of the reference on privacy being conducted by the Australian Law Reform Commission (ALRC). In December 2008, PIAC made a submission in response to the NSW LRC's *Consultation Paper 3: Privacy Legislation in NSW*.[5]

PIAC Chief Executive Officer, Robin Banks, is a member of the Privacy Advisory Committee (PAC), which provides strategic advice to the Federal Privacy Commissioner on privacy issues and the protection of personal information.

General Comments

This submission

PIAC congratulates the Federal Government on its speedy action to implement key aspects of the ALRC *Report 108 - For Your Information: Australian Privacy Law and Practice*[6] (Report 108) and its willingness to seek further input from key stakeholders prior to developing draft legislation.

PIAC has sought to keep this submission on the draft Unified Privacy Principles (UPPs) short and, where appropriate, has provided a page reference to its submission in response to DP 72 to enable the reader to refer to the original arguments made in support of a particular position.

PIAC has had the opportunity to review the submission of the Cyberspace Law and Policy Centre (CLPC) and has referred to its comments and amendments where appropriate.

Clarity of obligations and rights

PIAC submits that the Federal Government should be seeking to ensure that the amendments result in greater clarity and accessibility in terms of both rights and obligations. At its core, the proposal to establish the UPPs is a mechanisms that seeks to do this.

---

1 Emma Golledge and Carol Berry, *Health and Social Services Access Card: Submission to Access Card Consumer and Privacy Taskforce, Discussion Paper 1* (2006); Carol Berry, *Health and Social Services Access Card: Comment on exposure draft of Human Services (Enhanced Service Delivery) Bill 2007* (2007); Carol Berry and Robin Banks, *Health and Human Services Access Card: Discussion paper 3 – Registration* (2007); Carol Berry, *Access Card Proposal Still Fails Public Interest Test: Comment on the Exposure Drafts of the Access Card Legislation* (2007). PIAC submissions are available on its website at < http://www.piac.asn.au/publications/pubs/dateindex.html>.

2 Robin Banks, Patricia Ranald and Anne Mainsbridge, *Submission to the Australian Bureau of Statistics on* Enhancing the Population Census: Developing a Longitudinal View (2005); Robin Banks, Patricia Ranald and Anne Mainsbridge, *Further Submission to the Australian Bureau of Statistics on its Discussion Paper* Enhancing the Population Census: Developing a Longitudinal View (2005).

3 Anne Mainsbridge, *Matching Rights with Remedies: a statutory cause of action for invasion of privacy, Submission to the NSW Law Reform Commission on Consultation Paper 1 – Invasion of Privacy* (2007).

4 Anne Mainsbridge with Robin Banks, *Resurrecting the right to privacy. Response to the Australian Law Reform Commission* Discussion Paper 72: Review of Australian Privacy Law (2007).

5 Public Interest Advocacy Centre, *Improving clarity and enhancing protection of privacy rights: Response to the NSW Law Reform Commission's* Consultation Paper 3: Privacy Legislation in NSW (2008).

6 Australian Law Reform Commission, *Report 108 – For Your Information: Australian Privacy Law and Practice* (2008).

One thing that interferes with clarity and accessibility is enactment of aspects of the rights or obligations in subordinate legislation. Another is the separation of related rights or obligations or important clarifications or limits on rights within the legislative instrument in such a way as to make it difficult to interpret those rights or obligations without legal training.

Many aspects of this submission are premised on the need to ensure the drafting of the UPPs achieves maximum clarity and accessibility of privacy rights and obligations.

Paramountcy of Unified Privacy Principles

PIAC submits that there should be no scope for regulatory provisions that derogate from the UPPs.

In the event that the Federal Government rejects this approach, PIAC submits that the legislation should require that where a derogation from the UPPs is considered necessary and appropriate in particular circumstances or for a particular agency or organisations this should be subject to the full scrutiny afforded to legislation, rather than the lesser scrutiny of subordinate legislation.

Further, for clarity and accessibility purposes any such derogations should be required to be included in the Privacy Act immediately following the UPPs and clearly identified as exceptions to the UPPs.

Co-extensive coverage of agencies and organisations

PIAC supports the approach taken in the UPPs of having co-extensive obligations for agencies and organisations and submits that it should be reflected in all of the UPPs.

Direct marketing by agencies: UPP 6

PIAC notes that UPP 6 is not applied to agencies and submits this should be amended as there may be development over time of the use of direct marketing by agencies, particularly those that are corporatised.

Use of identifiers by agencies: UPP 10

Similarly, PIAC notes that UPP 10 is not applied to agencies and submits that this too should be amended. PIAC refers the Department to the precedent in both the *Information Privacy Act 2000* (Vic) and the *Health Records and Information Privacy Act 2002* (NSW):

> Information Privacy Principle 7: Unique Identifiers[7]
>
> 7.1. An organisation[8] must not assign unique identifiers to individuals unless the assignment of unique identifiers is necessary to enable the organisation to carry out any of its functions efficiently.
>
> 7.2. An organisation must not adopt as its own unique identifier of an individual a unique identifier of the individual that has been assigned by another organisation unless-
>
> (a) it is necessary to enable the organisation to carry out any of its functions efficiently; or
>
> (b) it has obtained the consent of the individual to the use of the unique identifier; or

---

7 *Information Privacy Act 2000* (Vic), Sch 1.

8 'Organisation' in this Act refers to public sector organisations covered by the Act and, therefore, has a similar meaning in terms of government entities as 'agencies' in the Privacy Act.

(c) it is an outsourcing organisation adopting the unique identifier created by a contracted service provider in the performance of its obligations to the organisation under a State contract.

7.3. An organisation must not use or disclose a unique identifier assigned to an individual by another organisation unless-

(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the other organisation; or

(b) one or more of paragraphs 2.1(d) to 2.1(g) applies to the use or disclosure; or

(c) it has obtained the consent of the individual to the use or disclosure.

7.4. An organisation must not require an individual to provide a unique identifier in order to obtain a service unless the provision of the unique identifier is required or authorised by law or the provision is in connection with the purpose (or a directly related purpose) for which the unique identifier was assigned.

Health Privacy Principle 12: Identifiers[9]

(1) An organisation may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the organisation to carry out any of its functions efficiently.
(2) Subject to subclause (4), a private sector person may only adopt as its own identifier of an individual an identifier of an individual that has been assigned by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:
    (a) the individual has consented to the adoption of the same identifier, or
    (b) the use or disclosure of the identifier is required or authorised by or under law.
(3) Subject to subclause (4), a private sector person may only use or disclose an identifier assigned to an individual by a public sector agency (or by an agent of, or contractor to, a public sector agency acting in its capacity as agent or contractor) if:
    (a) the use or disclosure is required for the purpose for which it was assigned or for a secondary purpose referred to in one or more paragraphs of HPP 10 (1) (c)-(k) or 11 (1) (c)-(l), or
    (b) the individual has consented to the use or disclosure, or
    (c) the disclosure is to the public sector agency that assigned the identifier to enable the public sector agency to identify the individual for its own purposes.
(4) If the use or disclosure of an identifier assigned to an individual by a public sector agency is necessary for a private sector person to fulfil its obligations to, or the requirements of, the public sector agency, a private sector person may either:
    (a) adopt as its own identifier of an individual an identifier of the individual that has been assigned by the public sector agency, or
    (b) use or disclose an identifier of the individual that has been assigned by the public sector agency.

PIAC submits that the appropriate obligation on agencies under UPP 10 should be:

An agency may only assign its own unique identifiers to individuals if the assignment of identifiers is necessary to enable the organisation to carry out its functions.

An agency must not, unless otherwise expressly required or permitted under law, adopt as its own identifier of an individual an identifier of the individual that has been assigned:

9 *Health Records and Information Privacy Act 2002* (NSW), Sch 1.

(a) by another agency;
(b) an agent of another agency acting in its capacity as an agent;
(c) a contracted service provider under a Commonwealth contract with another agency where the contracted service provider is acting in that capacity;
(d) an Australian state or territory agency.

This provides for an objective test of necessity and removes the very broad notion of 'efficiently'. To permit efficiency to be a justification of the assignment of identifiers by agencies is overly permissive and there is no apparent basis for having a more permissive regime for agencies than for organisations.

It also prevents the use of a common identifier across agencies without express legislative permission to do so. This means that any proposal for shared identifiers across government agencies would be subject to parliamentary scrutiny.

Consent

Throughout the UPPs, the term 'consent' is used.[10] PIAC submits that this should, wherever it occurs in the UPPs, be amended to require 'express and informed' consent.

Authorised by or under law

Similarly, throughout the UPPs, the term 'authorised by or under law' or similar is used as a permissive term. PIAC submits that, in order to limit the inappropriate use of this permission, the term should be amended throughout to read 'expressly authorised by or under law'.

Cumulative requirements or alternatives

PIAC notes that throughout the UPPs there are sub-clauses that set out requirements that need to be satisfied either cumulatively or alternatively. That is, in some cases sub-clauses must all be satisfied, while in others, the head requirement can be satisfied through compliance with just one of the sub-clauses. The failure to include 'and' or 'or' at the end of each sub-clause (or sub-sub-clause) makes the UPPs less easy to follow.

An example of this is UPP 5.1, which has eight sub-clauses, many of which have sub-sub-clauses. Sub-clause (a) is quite clear in its draft internally as it states that 'both' must apply and uses the word 'and' between the two sub-sub-clauses. However, in order to understand whether one must satisfy all of the conditions set out in the sub-clauses in 5.1, one must go to the end of sub-clause (g), where the word 'or' indicates that satisfaction of only one of the sub-clauses is necessary.

PIAC submits that, for ease of reading and understanding, the relevant word 'and' or 'or' should be included at the end of every sub-clause (and every sub-sub-clause) to make it clear whether all or only one must be satisfied.

Information in possession or control

Current IPPs 4 to 9, which deal with agencies and personal information, are extended by operation of section 15 of the Privacy Act in their scope to cover personal information in the possession or control of an agency. Under the UPPs, this scope is reduced and, as a result, the obligations on agencies, and the

[10] See, for example, UPP 2.5(a), UPP 5.1(b), UPP 6.2(a)(i), IPP 11.1(b). PIAC notes that UPP 11.1(b) requires the person to be informed of the consequences of consenting in respect of their loss of rights.

protection of personal information in the control of government, is reduced. PIAC submits that such a reduction in protection should not result from the introduction of the UPPs and urges the Government to consider amendments to ensure the current level of protection of personal information in respect of agencies is maintained.

Comments on each UPP

UPP 1: Anonymity and Pseudonymity

PIAC strongly supports UPP 1, but seeks an amendment to limit the use of 'practicable' as a means to avoid the obligation.

The draft reflects changes to the DP 72 draft to strengthen the obligation and to remove the potential for confusion that was reflected in the inclusion of the term—in respect of pseudonymity—'provided this would not be misleading' in the DP 72 draft. Both of the changes that have been made from the DP 72 draft were the subject of advocacy in PIAC's submission on DP 72.[11]

PIAC reiterates its concerns from that earlier submission that the notion of 'practicable' needs to be constrained. To this end, PIAC urges that consideration be given to amending UPP 1 as set out below to ensure that agencies and organisations consider the obligation to offer anonymity and pseudonymity at the time of system design to ensure that the practicability of fulfilling this obligation is not undermined by poor system design:

> Organisations and agencies must design information systems to facilitate the observance of UPP 1.

UPP 2: Collection[12]

PIAC supports the establishment of UPP 2 and makes the following comments on aspects of the proposed principle:

- the clarity of drafting;
- the addition of the word 'reasonable' in respect of destruction of unsolicited information in UPP 2.4(a);
- the retention of the limit on the obligation in UPP 2.4 to unsolicited information from a third party;
- the removal of the requirement that a threat be 'imminent' as well as serious in UPP 2.5(c);
- the absence of an effective mechanism to allow for non-university social research in UPP 2.5(f).

PIAC supports the amendment UPP 2.1 to create an objective test, as this is more appropriate than the subjective test in the DP 72 draft, which required only a 'reasonable belief that the information is necessary for one or more of its functions or activities'.

Clarity of drafting

There are several aspects of the drafting of UPP 2 about which PIAC is concerned about or seeks to provide comment.

Firstly, any reference to functions or activities, such as in UPP 2.1, should refer to lawful functions and activities.

---

11 Mainsbridge and Banks, above n4, 47.

12 Ibid, 48.

Second, UPP 2.1 should be amended to make it clear what the necessity relates to. As currently drafted, it could relate to either the need for the personal information for one or more of an agency or organisation's functions or activities or the need for the collection.

It may be appropriate that the provision retain this flexibility or for that dual interpretation to be expressly permitted as there are collection obligations that are imposed by government on non-government organisations (such as in respect of significant financial transactions, and of government funding reporting[13]) where the personal information collected is not needed for the organisation's own functions or activities, but the collection is needed to satisfy those obligations.

Third, the use of the phrase 'the individual to whom the information concerns' is extremely unclear. It is used, for example, in UPP 2.5(c) and UPP 2.5(d)(ii). An alternative would be 'the individual the information is about' or 'the individual the information relates to' or 'the individual to whom the information relates'. Of these, the first is preferred as it is plainer language.

Reasonableness of destruction

UPP 2.4(a) constrains the requirement to destroy unsolicited personal information to destruction 'if lawful and reasonable t do so'. While the term 'lawful' is be relatively clear, it is not apparent when it might not be reasonable to destroy such information.

PIAC has previously raised concerns about the potential destruction of documents containing personal information where the person concerned may not be aware of those documents or their content. An example of this is historic documents held by either agencies or organisations in relation to the removal of Aboriginal and Torres Strait Islander children from their families or to the payment (or otherwise) of wages and other monies to a relevant authority to be held in trust for individual Aboriginal people. These latter documents have become vital to establishing a debt owed by the state to individuals and it would not, in that circumstance, be reasonable that they be destroyed until the person concerned or their descendants have been given an opportunity to consider the documents and either copy them or be provided with the originals.

PIAC suggests that consideration be given to amending the UPPs to require that the receipt of unsolicited personal information from a third party should always be notified to the person(s) and they be given a right of access and, at minimum, copying where the personal information is provided to the agency in some recorded form.

Application to unsolicited personal information generally

There should also be provision in UPP 2 to cover the situation where an agency or organisation receives unsolicited personal information from the individual. As currently drafted, UPP 2 is silent on this.[14] It may be sufficient to amend add a new paragraph to UPP 2 to the following effect:

> If an agency or organisation receives unsolicited personal information about an individual from that individual, it must 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.

---

13 An example is the personal information about advice and casework clients that must be collected by community legal centres under funding arrangements with state and Commonwealth governments and provided on a monthly basis to the funding administrator.

14 Mainsbridge and Banks, above n4, 49.

Absence of the requirement of imminence from UPP 2.5(c)

PIAC is opposed to the absence of the requirement that a threat be imminent as well as serious in UPP 2.5(c).[15] As drafted, UPP 2.5(c) may allow an agency to collect sensitive information about a person without their consent on the basis that this information might be necessary to prevent a serious threat to their life or health at some time in the future. The requirement that a threat be imminent as well as serious indicates that there must be some degree of urgency and, as a result of that urgency, limited access to other mechanisms available to prevent the threat eventuating.

In PIAC's view, the requirement of imminence operates as an important safeguard. If the exception can be triggered simply when a threat is 'serious' it could be used to justify collection of sensitive information without consent on the basis that the information could prevent some future serious harm.

Of particular concern is the impact of the permissive wording on people with mental illness, where there may be a potential for serious threat to health, but no imminence, because at the relevant time the illness is well controlled by medication or is episodic and the person is not currently unwell. Where a person is currently well they are in a better position to consent to the collection if they can be persuaded that it could prevent a future harm.

Where a person is temporarily unwell and unable to consent then the threat should be imminent in order to permit collection as this would protect against the potential for information to be prematurely collected at a time a person is unwell and unable to consent but the threat is not, at that time, otherwise avoidable.

As with the example cited above, where the threat is serious but not imminent other mechanisms should be utilised to avoid the threat eventuating without recourse to non-consensual collection of sensitive information.

Non-university research involving sensitive information

PIAC is concerned about the impact of UPP 2.5(f) on non-university research. PIAC, like many other organisations, seeks to use case studies to illustrate policy or law reform proposals. Sometimes, those case studies will include sensitive information. While in some cases the individual concerned may have consented, in other cases it may not be possible to obtain consent because the case study is provided by a third party organisation and they are no longer able to identify or contact the person.[16] In that case, UPP 2.5(f) would be the appropriate one to refer to and so all of the conditions must be satisfied. While it may be relatively easy to satisfy paragraphs (i) and (ii), and possible to satisfy paragraph (iv), the establishment of a Human Research Ethics Committee by a small entity for the purposes of a single research report would be difficult if not impossible to achieve meaningfully.

While it has been suggested that, in such a case, UPP 2.5(d) would apply, this would not assist as many such research reports involve using cases studies that arise from one-off contact with an individual.

PIAC does not seek to reduce the privacy protection, particularly in relation to sensitive information. PIAC would welcome the opportunity to work further on this issue with the Government and others to establish

---

15 Ibid, 50.

16 An example is PIAC's report on the impact of the on-the-spot fine system in NSW on homeless people and others facing disadvantage, *Not such a fine thing! Options for Reform of the Management of Fines Matters in NSW* (2006). This report uses case studies to highlight some of the key impacts and was a major tool in PIAC's successful campaign to have the law and procedures in NSW reformed. PIAC is also aware of government agencies that undertake or commission research that would be affected by this provision.

an effective mechanism to ensure important research can continue to be done and used as the basis of policy development and change.

UPP 3: Notification

PIAC supports the establishment of a separate notification principle and commends the ALRC on the inclusion of notification regarding the right to correction in UPP 3(c).[17]

PIAC is concerned to ensure that the circumstances in which post-collection notification is permitted are constrained. The current use of the term 'practicable' is inappropriately permissive as an organisation may assert, for example, that it wasn't practicable to include information about collection through an RFID tag at the point of collection due to space constraints or lack of staff understanding of the collection mechanism. However, it is even less practicable to notify after collection in such a case.

PIAC supports the amendment proposed to UPP 3(b) by the Cyberspace Law and Policy Centre (CLPC).

UPP 4: Openness

PIAC supports the text of UPP 4 and the additional sub-clauses to UPP 4.1 and the new UPP 4.3 proposed by the CPLC.

In relation to UPP 4.2(b), PIAC suggests that the UPP or guidance in relation to the UPP should make it clear that no charge should be made to provide an alternative form of the policy if there is no charge made to access the electronic copy.[18] To do otherwise would potentially be unlawfully discriminatory under the *Disability Discrimination Act 1992* (Cth), as it would treat a person who required an alternative form of the policy because of disability less favourably. Further, there should not be any delay in providing the policy in an alternative form because a delay could reduce the efficacy of the provision of the policy.

PIAC also notes that such guidance should make it clear that provision of the policy in the electronic format of PDF is not generally accessible to people with vision impairment and would not be sufficient to satisfy the 'alternative form' requirement.

UPP 5: Use and Disclosure[19]

PIAC generally supports the text of UPP 5, with three qualifications:

- retention of requirement of imminence in relation to serious threats;
- use or disclosure for non-university research; and
- interpretative aids.

Retention of the requirement of imminence

PIAC submits that UPP 5.1(c) should retain the requirement of 'imminence' through amending the text to read 'necessary to lessen or prevent a serious and imminent threat'.[20] An alternative is the wording proposed by the CLPC. However, PIAC submits that for the sake of clarity, the order of CLPC's sub-clauses (i)

---

17 Mainsbridge and Banks, above n4, 52.

18 For the reasons outlined above in the General Comments section, PIAC submits that an amendment to the UPP itself is to be preferred to provide this clarity.

19 Mainsbridge and Banks, above n4, 56.

20 Mainsbridge and Banks, above n4, 50.

and (ii) should be reversed to make it absolutely clear that the additional condition that commences 'and there is an urgent need …' applies to a 'serious threat to an individual's life, health or safety'.

Use or disclosure for non-university research

PIAC reiterates its comments above under UPP 2 above in relation to non-university research. The requirements in UPP 5.1(g) must all be satisfied and in PIAC's experience would be extremely difficult if not impossible for a non-university research or policy organisation to satisfy without prohibitive cost. Consideration needs to be given to alternative mechanisms for ensuring appropriate protection of personal information being used for policy development and research purposes.

Interpretive aids

PIAC has repeatedly identified the need to ensure that the law is clear on its face so as to avoid people having to understand the rule of legislative interpretation, such as the option of using Explanatory Memorandum as an aid to interpretation in the case of ambiguity. CLPC has suggested in its comments at the end of UPP 5 that the Explanatory Memorandum to the enacting legislation could confirm, for example, that accessing information without anything further is 'use' for the purposes of this UPP. PIAC submits that the three clarifications sought by CLPC should be provided within the legislation. Indeed, these should be included in UPP 5. The fourth clarification proposed should also be found in UPP 5.

Subject to the comments made above, PIAC endorses the amendments proposed and comments made by the CLPC.

UPP 6: Direct Marketing[21]

As noted above, PIAC believes that the Direct Marketing principle should not be limited in its application to organisations; It should extend to agencies. PIAC's other concerns relate to the use of sensitive information and the application of the principle to non-customers and those under 15 years of age.

Sensitive information

The current drafting appears, by implication, to permit the use of sensitive information for direct marketing without any limits if the individual is an existing customer or aged 15 years or over. PIAC submits that the use and disclosure of sensitive information for direct marketing should be seriously constrained, if permitted at all; and not be permitted in relation to those under the age of 15 years or for non-customers, with perhaps an exception in circumstances where agencies have a legitimate and pressing reason for communicating information to individuals, eg, targeted public health and safety campaigns.

Under UPP 6.2(a), direct marketing that involves the use or disclosure of sensitive information in relation to non-customers and individuals under 15 years of age is permitted with consent. Given the serious potential consequences of use or disclosure of sensitive information and the limited capacity of juveniles to understand long-term consequences, permitting the use of sensitive information with consent of the individual (informed or otherwise) is problematic.

Further, in the case of non-customers and individuals under 15 years of age it is difficult to imagine how an organisation would have obtained sensitive information without a breach of another UPP by either the organisation or another organisation or agency.

---

21 Mainsbridge and Banks, above n4, 57.

Individuals under 15 years of age and non-customers

All of the discussions PIAC has been involved in respect of direct marketing seem to take as a given that direct marketing is going to be undertaken to individuals under 15 years of age and that this is either okay or positive. PIAC challenges the presumption implicit in this provision that direct marketing to individuals under 15 years of age should be permitted.

While acknowledging the difficulty of ascertaining an individual's age, PIAC believes that the fact an organisation has other personal information sufficient to undertake direct marketing, including potentially sensitive information about the individual, suggests it would be possible to ascertain from the individual their age before any direct marketing is undertaken.

Similarly, it is difficult to imagine a situation where an organisation is seeking to undertake direct marketing to a non-customer or person under the age of 15 but where it is impracticable for the organisation to seek the individual's consent as is permitted under UPP 6.2(a)(ii). If sufficient personal information is held to conduct direct marketing, then sufficient details must be available to enable contact with the individual for the purpose of obtaining consent before any direct marketing is undertaken.

The other aspect of direct marketing to non-customers and minors about which PIAC has concerns is the limit on the requirement to disclose the source of personal information is UPP 6.2(d). PIAC submits that the requirement to disclose the source of the individual's personal information should be unconditional. It should always be reasonable and practicable for the organisation to disclose the source of the information and, as such, the words 'where reasonable and practicable' should be removed.

UPP 7: Data Quality[22]

PIAC submits that the burden of ensuring the accuracy, completeness, currency and relevance in relation to sensitive information should be set higher than for other information.

PIAC also urges the Government to consider further the extension of UPP 7 to information not only in the possession of an agency or organisation, but also in its control.[23] The omission of this from UPP 7 reduces the obligations that currently exist on agencies under IPP 8. PIAC considers the discussion of this aspect in Report 108 does not sufficiently deal with the potential for data quality to be outside any entities' responsibility where storage, etc, is outsourced. PIAC notes that the ALRC suggests that to 'extend[…] the data quality principle in this way would impose an unjustified compliance burden on agencies and organisations'.[24] While it may impose an additional compliance burden on organisations, there is no additional burden on agencies and the adoption of UPPs should not see a reduction in protection in respect of personal information held by government.

UPP 8: Data Security[25]

PIAC endorses the comments of and amendments proposed by the CLPC. In particular PIAC is concerned the ensure that the security of data disclosed to third parties under contractual arrangements is maintained.[26] The obligations should remain on the entity with whom the individual has had direct dealings, be it an agency or organisation, to ensure that the individual can take action against that agency

22 Ibid, 59.
23 Ibid.
24 ALRC, above n6, 937.
25 Ibid, 60.
26 Ibid, 60-61.

or organisation for any breach rather than having to ascertain the identity, location, etc, of the contracting third party in order to seek a remedy for a breach.

In addition, PIAC against urges that consideration be given to requiring the individual concerned to be informed prior to destruction to ascertain whether or not the individual seeks to retain the original or a copy of the personal information. As noted in PIAC's submission on DP 72, personal information should not be destroyed where, for example, the individual concerned may thereby lose access to evidence that would support a legal claim.[27]

UPP 9: Access and Correction[28]

PIAC endorses the comments of and amendments proposed by the CLPC.

As with UPP 4 above, PIAC submits that a note or amendment should be made to UPP 9.4 and 9.5 to ensure access to personal information is provided at no additional charge in an accessible format to a person who requires an alternative format because of disability. The limit on the obligation in UPP 9.5 created by the inclusion of the term 'where reasonable and practicable' could very easily result in unlawfully discriminatory limits on access both in terms of format of information and in terms of any requirement to travel to a particular location to access that information. PIAC accepts, however, that there should be a limit to the obligation to provide access in the manner requested to situations where the request is reasonable. The proposed note or amendment should indicate that a request for a particular manner of access because of disability should be presumed to be reasonable.

UPP 10: Identifiers[29]

See comments above under General Comments: Co-extensive coverage of agencies and organisations: Use of identifiers by agencies.

UPP 11: Cross-border Data Flows[30]

PIAC is extremely disappointed with UPP 11 as it fails to provide appropriate and adequate protection against or recourse and remedy for failure to ensure the privacy of personal information.

To begin, PIAC notes that, other than in the heading of the UPP, UPP 11.1 does not expressly refer to transfer of data across a border, or the nature of that border. It should be made clear in the UPP that is deals with the transfer of personal information outside of Australia and its external territories.

PIAC submits that, other than the exception provided for in UPP 11.1(c) (as amended by the CLPC), there should be no exceptions to an agency or organisation remaining accountable for personal information that it transfers across a border.

The amendments proposed by the CLPC do not address PIAC's concerns that an individual should not have to take action in another jurisdiction against a third party in order to protect the rights afforded by Australian privacy law. An individual should always be able to seek a remedy in Australia for a breach of privacy relating to personal information where that breach occurred in relation to personal information that had been transferred outside Australia by an agency or organisation. And the individual should always be

27 Ibid, 61-62.
28 Ibid, 61-64.
29 Ibid, 64-65.
30 Ibid, 66-69.

able to take the action against the entity with which he or she had direct dealings, that is the Australian agency or organisation to whom the individual disclosed personal information.

PIAC believes that this approach, whereby accountability remains with the agency or organisation, is a much simpler and straightforward approach. PIAC supports the proposal set out in UPP 11.2 that the Privacy Commissioner be empowered to make the determinations about the adequacy of privacy protections in other jurisdictions as this may provide guidance to agencies and organisations about privacy matters before determining whether or not to engage in cross-border data transfer.

Additional principles

PIAC endorses the comments and proposed drafting from the CLPC in relation to a new UPP dealing with Data Breach Notification or an amendment to UPP 8.

PIAC also endorses the comments and proposed drafting from the CLPC in relation to a new UPP prohibiting the imposition of a cost or other burden on an individual who seeks to enjoy the rights conferred by the UPPs.