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

Best practice privacy principles: suggested improvements to the ALRC's model unified privacy principles (UPPs)

Submission to the Australian Government

Nigel Waters & Graham Greenleaf

30 December 2008

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

Graham Greenleaf
Professor of Law
University of New South Wales

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

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

We welcome the ALRC's recommendations for unified privacy principles (UPPs), to apply both to Commonwealth agencies and to private sector organisations under an amended Privacy Act 1988. We also support the ALRC's call for State & Territory governments to adopt the UPPs in their own legislation, to create a simpler and more effective privacy protection regime for all Australians.

The ALRC has, undersandably, drafted some of its proposed UPPs as a compromise between different viewpoints submitted by stakeholders. This has, in our view, led to some of the UPPs not being practicable or operationally efficient. In other respects, we believe the proposed UPPs to be weaker than the existing principles (IPPs or NPPs) – an outcome which we don't think the government intended, and which the Australian public would certainly not welcome. We believe that the UPPs should represent international best practice in privacy protection, and address some of the manifest weaknesses in the existing principles and the way in which they have been implemented and interpreted.

We therefore submit our suggested amendments to the UPPs, with our reasons. We have tried to mimimise the extent of any differences from the ALRC proposals, as we understand the desirability of following the ALRC model as closely as possible as the foundation for a new regime, especially after such extensive consultation and consideration.

This submission contains suggestions only for the proposed UPPs. We submit that there are a number of related recommendations from the ALRC relating to enforcement powers and complaint handling which need to be implemented at the same time (i.e. in the first stage of legislation), if the new principles are to achieve their objective. Unlike the ALRC, we also submit that some amendments to core definitions, such as 'personal information' are necessary to ensure the technological neutrality and overall effectiveness of the Act. We will be making a separate submission about these other necessary changes.

The format of this submission is a table, setting out firstly the ALRC's proposed UPP, followed in the second column by our commentary, and in the third column, our suggested 'improved' UPP. At the end, we include two additional UPPs – on data breach notification, and a 'no-disadvantage' principle.

References in the 'Comments' column to 'CLPC72' are to the Centre's December 2007 submission on the Privacy Principles part of the ALRC's Discussion Paper 72, and references to 'CLPC IP31' are to the Centre's January 2007 submission on the ALRC's Issues Paper 31.
(both at http://www.cyberlawcentre.org/ipp/publications.html)

ALRC Model UPP	Commentary	Suggested UPP
UPP 1. Anonymity and Pseudonymity	***Comments***	*UPP 1. Anonymity and Pseudonymity*
Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:	• We support the reformulation of UPP1 to state that agencies and organisations must give individuals the option of anonymity/pseudonymity, not that 'individuals … should have' this option. (p. 13, CLPC72).	1.1 Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:
(a) not identifying themselves; or		(a) not identifying themselves; or
(b) identifying themselves with a pseudonym.		(b) identifying themselves with a pseudonym.
	• 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 (p. 14, CLPC72). • 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). If NPP 8 had required telcos to facilitate the ability for subscribers to remain anonymous in their interaction with third parties then it would have been possible to argue that charging for silent lines breached the principle. (p. 14, CLPC72).	1.2 Agencies and organisations responsible for specifying the design of and information system in which it can be reasonably anticipated that personal information will be held either by the agency or organisation itself or by a third party must ensure that, wherever it is lawful and practicable in the circumstances, the design of the information system gives individuals the clear option of interacting with the third party by either: (a) not identifying themselves; or (b) identifying themselves with a pseudonym.

UPP 2. Collection	*Comments*	*UPP 2. Collection*
2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.	• The test needs to go to the reasonableness of the purpose rather than merely the reasonableness of information collection in the context of whatever functions or activity the organisation/agency specifies (p. 18, CLPC72). • 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 (p. 18, CLPC72). • 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 principle should make it clear that collection can only be for a lawful purpose (p. 18, CLPC72).	2.1 An agency or organisation must not collect personal information unless it is necessary for one or more of its lawful functions or activities and the particular purpose of collection, and is proportional to those functions or activities and particular purpose.
2.2 An agency or organisation must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.		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.		2.3 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 receives unsolicited personal information about an individual from someone else, it must either:		2.4 If an agency or organisation receives unsolicited personal information about an individual from someone else, it must either:
(a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or		(a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the

disclosing it except for the purpose of determining whether the information should be retained; or		purpose of determining whether the information should be retained; 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.		(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.
2.5 In addition to the other requirements in UPP 2, an agency or organisation must not collect sensitive information about an individual unless:		2.5 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;	• 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 (p. 19, CLPC72). The other exceptions are designed to deal with situations where express consent is not practicable.	(a) the individual has expressly consented;
(b) the collection is required or authorised by or under law;	• The proposed exception for collection that is required or 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 strongly support the inclusion of 'specifically authorised' in UPP 2.6(b) (p. 19, CLPC72). This will still be more permissive thand NPP10, but less so than the ALRC's very broad exception.	(b) the collection is required or specifically authorised by or under law;
(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving	• 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 also be 'imminent'. In the context of this principle (as	(c) the collection is necessary to prevent or lessen a serious threat to the life or health of any individual, where the individual to whom the information concerns is legally or physically incapable of giving or communicating consent;

or communicating consent;	with UPP 9), we agree with this change – in contrast to our position on UPP 5 see below. This difference reflects the inclusion in UPP 2.5(c) of an additional test – that consent not be an option, and the fact that this is dealing specifically with sensitive information.	
(d) if the information is collected in the course of the activities of a non-profit organisation—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 to whom the information concerns that the organisation will not disclose the information without the individual's consent;	• 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 [involved in] unlawful discrimination, race hate etc (p. 19, CLPC72).	(d) the information is collected in the course of the lawful activities of a non-profit organisation which requires the sensitive information for the fulfilment of its purposes and 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 to whom the information relates that the organisation will not disclose the information without the individual's consent;
(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;		(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim;
(f) the collection is necessary for research and all of the following conditions are met: (i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable; (ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection; (iii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the National Statement on Ethical Conduct in Human Research (2007), as in force from time to time, has reviewed the proposed activity and		(f) the collection is necessary for research and all of the following conditions are met: (i) the purpose cannot be served by the collection of information that does not identify the individual or from which the individual would not be reasonably identifiable; (ii) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection; (iii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the National Statement on Ethical Conduct in Human Research (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that

is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act; and (iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or		the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the Privacy Act; and (iv) the information is collected in accordance with Research Rules issued by the Privacy Commissioner; or
(g) the collection is necessary for the purpose of a confidential alternative dispute resolution process.	• To ensure that this exception is only available to bona fide ADR schemes, we submit that it should only apply to prescribed schemes. A Regulation making power should provide for minimum criteria, to include appropriate confidentiality provisions. We anticipate that the Regulations would prescribe at least those ADR schemes already approved by ASIC.	(g) the collection is necessary for the purpose of a prescribed alternative dispute resolution process.
2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.		2.6 Where an agency or organisation collects sensitive information about an individual in accordance with 2.5(f), it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.
Note: Agencies and organisations that collect personal information about an individual from an individual or from someone else must comply with UPP 3.	We submit that this cross reference should appear in Guidance rather than in the UPP itself. Inclusion of some specific compliance reminders runs the risk of omitting others that are equally significant	

UPP 3. Notification	*Comments*	*UPP 3. Notification*
3. 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 or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify the individual, or otherwise ensure that the individual is aware of, the:	• 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(a) and also on these different modes of collection in relation to UPP 2) (p. 27, CLPC72).	3. 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 by any means other than collection of publicly available information it must take such steps, if any, as are reasonable in the circumstances to notify the individual or otherwise ensure that the individual is aware,, of the:
(a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;	• 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 (p. 29, CLPC72).	(a) fact and circumstances of collection, where the individual may not be aware that his or her personal information has been collected;
(b) identity and contact details of the agency or organisation;	• We support the inclusion of these details, to apply to both agencies and organisations (UPP 3(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 (p. 29, CLPC72).	(b) identity and functional contact details of the agency or organisation;
(c) rights of access to, and correction of, personal information provided by these principles;	• We support the inclusion of item (c) in UPP 3 and, in particular, the inclusion of a requirement to notify individuals of the important right to seek correction (p. 29, CLPC72).	(c) rights of access to, and correction of, personal information provided by these principles;
(d) purposes for which the information is collected;	• We support the inclusion of items (d) and (e) in UPP 3, which are carried over from NPP 1.3 (in the latter case, with some desirable simplification) (p. 29, CLPC72).	(d) purposes for which the information is collected;

(e) main consequences of not providing the information;	• We support the inclusion of items (d) and (e) in UPP 3, which are carried over from NPP 1.3 (in the latter case, with some desirable simplification) (p. 29, CLPC72).	(e) main consequences of not providing the information;
(f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;	• We support the inclusion of information about usual disclosures as UPP 3(f) (p. 30, CLPC72).	(f) actual or types of organisations, agencies, entities or other persons to whom the agency or organisation usually discloses personal information of the kind collected;
(g) fact that the 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 are set out in the agency's or organisation's Privacy Policy; and	• We support the inclusion of item (g) in UPP 3 (p. 30, CLPC72).	(g) fact that the 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 are set out in the agency's or organisation's Privacy Policy; and
(h) fact, where applicable, that the collection is required or authorised by or under law.		(h) fact, where applicable, that the collection is required or authorised by or under law.

UPP 4. Openness	*Comments*	*UPP 4. Openness*
4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:		4.1 An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including how it collects, holds, uses and discloses personal information. This document should also outline the:
(a) sort of personal information the agency or organisation holds;		(a) sort of personal information the agency or organisation holds;
(b) purposes for which personal information is held;		(b) purposes for which personal information is held;
(c) avenues of complaint available to individuals in the event that they have a privacy complaint;		(c) avenues of complaint available to individuals in the event that they have a privacy complaint;
(d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and		(d) steps individuals may take to gain access to personal information about them held by the agency or organisation; and
(e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.	• We support this obligation very strongly, but consider its inclusion in a Privacy Policy is in itself inadequate to provide sufficient warning of the risks of such transfers. See our submission on UPP 11.	(e) whether personal information is likely to be transferred outside Australia and the countries to which such information is likely to be transferred.
	• The privacy policy should also include three other items of information currently required of agencies by IPP 5.3((c)-(e)	(f) the types of individuals about whom records are kept;
		(g) the period for which each type of record is kept; and

		(h) 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:	• 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 (p. 34, CLPC72).	4.2 An agency or organisation should take reasonable steps to make its Privacy Policy available without charge to an individual:
(a) electronically; and	• The electronic publication requirement should refer specifically to the Internet as the preferred channel of publication – the Internet is is now and for the foreseeable future such a universally available and accepted. platform that it is can no longer be regarded as technologically specific,	(a) electronically, including wherever reasonable and practicable, by publication on a publicly accessible Internet website; and
(b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.		(b) on request, in hard copy, or in an alternative form accessible to individuals with special needs.
	• 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). 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. This potential could be realised much more easily if the Commissioner used innovative ways of presenting the material and making it searchable/browsable. 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 (p. 34, CLPC72). We do not suggest extending this obligation to private sector organisations.	4.3 An agency must submit to the Privacy Commissioner at least once each year, an electronic copy of its privacy policy or the Internet address at which its privacy policy can be located.

UPP 5. Use and Disclosure	*Comments*	*UPP 5. Use and Disclosure*
5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (the secondary purpose) unless:		5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose other than the primary purpose of collection (a secondary purpose) 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;	• We support this proposed exception (p. 39, CLPC72).	(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;
(b) the individual has consented to the use or disclosure;	• We support this proposed exception (p. 39, CLPC72).	(b) the individual has consented to the use or disclosure;
(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;	• 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. (p. 40, CLPC72). • We oppose the deletion of the qualifying word 'imminent' from UPP 5.1(c)(i) (variation on submission at p. 40, CLPC72).	(c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent: (i) a serious threat to an individual's life, health or safety;or (ii) a serious and imminent threat to public health or public safety; and there is an urgent need for the use or disclosure such that any other means of compliance with this principle is not practicable in the circumstances.

	• It is essential to retain a test of 'urgency; to justify why another basis for use or disclosure cannot be established (e.g. obtaining lawful authority, or applying for a Public interest Determination).	
(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;	• We support the proposed exception UPP 5.1 (d). (p. 40, CLPC72).	(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;
(e) the use or disclosure is required or authorised by or under law;	• We support a narrowing of the proposed exception UPP 5.1 (e) to include 'specifically' as the ALRC proposed in DP 72.(p. 41, CLPC72). We note that the ALRC has changed its position on this in Report 108, but we are not persuaded by its reasons for doing so. 'Authorised' by law is simply too wide a concept and can and will be abused. The ALRC's contends that its proposed clarification of the meaning of 'law' (Recommendation 16-1) deals adequately with the issue. We disagree, as this recommendation is only for an illustrative, and not exhaustive, definition. • The ALRC suggests that including 'specifically' in the principle would necessitate a review of current legislationto ensure that, where needed, use and diclosure of personal information is specifically authorised. We submit that this would be a desirable outcome.	(e) the use or disclosure is required or specifically authorised by or under law;
(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;	• We support the proposed exception UPP 5.1 (f) (p. 41, CLPC72). We suggest that there should be a Note to this exception stating that it requires the active involvement of an Australian enforcement body. The ALRC says (at-25.118) : "The law enforcement exception should not be limited to circumstances in which there is an 'active' involvement of an enforcement body, as suggested by two stakeholders. Such a provision would be counter-productive, potentially limiting the operation of the law enforcement exception to allowing use and disclosure of personal information to assist law enforcement bodies to undertake existing investigations into offences and breaches of the law. A law enforcement body,however, may not be in a position to prevent, detect or investigate offences or breaches of the law, unless and until	(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

(iii) the protection of the public revenue; (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal;	certain information, including personal information, is brought to its attention. The exception, therefore, should not be framed in a manner that prejudices the ability of enforcement agencies to initiate investigations in the public interest." • This misrepresents the intent behind our earlier submission – we did not mean to suggest that an enforcement body had to initiate an investigation – merely that at some stage an enforcement body would have to be informed, and agree that there were grounds for continuing the investigation. This condition is necessary to prevent agencies and organisations making independent decisions about law enforcement matters for which they do not have the necessary competence. The 'by or on behalf of' condition in this exception should go some way towards limiting self serving interpretations, but we submit that a note would usefully re-inforce this limitation.	of seriously improper conduct or prescribed conduct; or (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; Note: This exception requires the active involvement, at an appropriate stage, of an enforcement body.
(g) the use or disclosure is necessary for research and all of the following conditions are met: (i) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure; (ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; (iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and (iv) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably	• This recommendation involves binding 'Rules' to be issued by the Privacy Commissioner. We refer to our general comments about the status and relationships between various instruments under the Privacy Act.	(g) the use or disclosure is necessary for research and all of the following conditions are met: (i) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure; (ii) a Human Research Ethics Committee that is constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* (2007), as in force from time to time, has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; (iii) the information is used or disclosed in accordance with Research Rules issued by the Privacy Commissioner; and (iv) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which

identifiable; or		the individual would be reasonably identifiable; or
(h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.		(h) the use or disclosure is necessary for the purpose of a confidential alternative dispute resolution process.
5.2 If an agency or organisation uses or discloses personal information under paragraph 5.1(f) it must make a written note of the use or disclosure.	• The ALRC concludes that the potential benefits of a general record-keeping requirement are outweighed by a disproportionate compliance burden. (Report 108, 25.183), and recommends only the continuation of the obligation relating to 'law enforcement' uses and disclosures (exception (f)) . We are very disappointed with this conclusion and submit that the requirement be imposed for exceptions (c)-(h). 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. (pp. 41-42, CLPC72). Secondary uses 'related ... and within reasonable expectations' (exception (a)) can be exempted from this specific requirement. So too can 'consent' (exception (b)), although imost agencies and organisations would probably find it prudent in any case to keep records to support a basis of consent.	5.2 If an agency or organisation uses or discloses personal information for a secondary purpose under any of the exceptions 5.1(c)-(h), it must make a written note of the use or disclosure with reasons.
5.3 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.		5.3 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 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.		Note 1: It is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions in the performance of their functions.
Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. Nothing in subclause 5.1 requires an agency or organisation to disclose	• We support this clear statement that all the exceptions are discretionary and are neither a requirement nor an authorisation to use or disclose (p.42, CLPC72).	Note 2: Subclause 5.1 does not override any existing obligations not to disclose personal information. Nothing in subclause 5.1 requires an agency or organisation to disclose

personal information; an agency or organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.		personal information; an agency or organisation is always entitled not to disclose personal information in the absence of a legal obligation to disclose it
Note 3: Agencies and organisations also are subject to the requirements of the 'Cross-border Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.	• While we do not generally favour cross references to other compliance obligations in the UPPs, we support this as an exception, as it would be easy to overlook the application of UPP11.	Note 3: Agencies and organisations also are subject to the requirements of the 'Cross-border Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.
	• 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 (p. 37 CLPC72). • 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 (p. 38, CLPC72). • 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' (p. 38, CLPC72). • The law should be clarified to expressly allow for the declaration of multiple specific purposes, but not to allow a broadly stated purpose (p. 39, CLPC72).	

UPP 6. Direct Marketing (only applicable to organisations)	*Comments*	*UPP 6. Direct Marketing*
6.1 An organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:	• We believe the principle should apply to both agencies and organisations 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 (p. 44, CLPC72).	6.1 An agency or organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where
(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and	• This principle has now lost the requirement (in NPP 2.1(c)) for the direct marketing to be 'related' to the primary purpose of collection. We accept this change – given that the essential 'reasonable expectation' test remains. We expect that this test would require an agency or organisation, if challenged, to demonstrate compliance by reference to customer surveys – merely showing that they had informed customers of their intentions would not suffice. • It is implicit that this exception would not allow marketing to individuals who expressly inform an agency or organisation that they do not wish to receive direct marketing communications , as the obligation under 6.3 (6.4 in our proposal) would prevail. • 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. A required ... by law	(a) the individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing, or (b) the use of information for direct marketing is required or specifically authorised by or under law,

	exception is necessary to allow for communication for existing customers who do not reasonably expect direct marketing, or who have opted out. Given the increasing delivery of government services through the private sector, such an exception should also apply to organisations (p. 45, CLPC72). It is self-evident that this exception must only be where the marketing is required or *specifically* authorised, as this would be the only justification for overriding indviduals' preferences.	
(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications.	• Condition (b) needs to apply to both 6.1 and 6.2, and should therefore stand alone – see below.	
6.2 An organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:	• We note that there may be practical difficulties in ascertaining an individual's age, and it would be undesirable for there to be collection of age information, where otherwise unnecessary, merely to assist compliance with this principle. If age verification is impracticable in many circumstances (as in Internet and SMS transactions) it may be better to impose a single rule on all direct marketing, perhaps allowing a lesser standard of implied consent for existing customers (this is after all another expression of 'reasonable expectation)? • We further note that some submissions have been made to the effect that the use of sensitive information for marketing, at least to juveniles and non-customers, should not be allowed at all. However, we do not think it should be a function of privacy law to prohibit particular forms or targets for direct marketing – unless that is indirectly the consequence of imposing reasonable conditions on the use of personal information for marketing.	6.2 An agency or organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:
(a) either the: (i) individual has consented; or (ii) information is not sensitive information and it is	• Unless the requirement is for 'express' consent, it will be possible for this limitation to be avoided by a range of techniques including 'bundled' consent and 'small print' options – relying on 'implied' consent (given the definition of consent in s.6).	(a) either the: (i) individual has expressly consented; or (ii) information is not sensitive information and it is impracticable for the organisation to seek the

impracticable for the organisation to seek the individual's consent before that particular use or disclosure;	• There is recent evidence that the inclusion of implied consent as a basis for exceptions to the Do Not Call List has undermined its effectiveness (see The Australia Institute Discussion Paper No 104 Go Away Please – the social and economic impact of intrusive marketing, December 2008). This flaw needs to be avoided here.	individual's consent before that particular use or disclosure; or
	• 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 (p. 45, CLPC72).	(b) the use of information for direct marketing is required or specifically authorised by or under law,
(b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;	• This condition needs to apply to both 6.1 and 6.2, and we therefore submit it should be part of a new 6.3	6.3. Where undertaking direct marketing in accordance with 6.1 or 6.2, an agency or organisation must (a) in each direct marketing communication, draw~~s~~ to the individual's attention, or prominently display a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications, and direct them to the means by which they may do so;
(c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and	• This condition needs to apply to both 6.1 and 6.2, and we therefore submit it should be part of a new 6.3	(b) provide a simple and functional means by which the individual may advise the agency or organisation that he or she does not wish to receive any further direct marketing communications. If the communication is by electronic means, the means of contact must be at least as easy to use; and
(d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.	• 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]). (p. 47, CLPC72). • This condition needs to apply to both 6.1 and 6.2, and we therefore submit it should be part of a new 6.3	(c) if requested by the individual, and where reasonable and practicable, the agency or organisation must advise the individual of the identity of the source from which it acquired the individual's personal information.

6.3 In the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:	I • ndividuals 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 (p. 47, CLPC72).	6.4 If an individual makes a request, either directly or indirectly, to an agency or organisation not to receive any further direct marketing communications, the agency or organisation must:
(a) comply with this requirement within a reasonable period of time; and		(a) comply with this requirement within a reasonable period of time; and
(b) not charge the individual for giving effect to the request.		(b) not charge the individual for giving effect to the request.

UPP 7. Data Quality	*Comments*	*UPP 7. Data Quality*
An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.	• If an agency or organisation uses or discloses personal information for a secondary purpose, then the appropriate question is whether the information is of a quality appropriate for that use or disclosure – we support the ALRC's inclusion of this in this principle (p. 50, CLPC72). • We also support the inclusion of 'relevant' as a criterion.	An agency or organisation must take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.
	• 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 (p. 49, CLPC72).	Note: 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 for individuals in the context of the particular information and circumstances.

UPP 8. Data Security	*Comments*	*UPP 8. Data Security*
8.1 An agency or organisation must take reasonable steps to:		8.1 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; and	• 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 (p. 51, CLPC72).	(a) protect the personal information it holds from improper access, use, alteration, deletion or disclosure, or other misuse, by both authorised users and by other parties; and
(b) destroy or render non-identifiable personal information if it is no longer needed for any purpose for which it can be used or disclosed under the UPPs and retention is not required or authorised by or under law.	• We support the objective of the ALRC's proposed UPP 8.1(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) (and p. 52, CLPC72). • However, the wording of the principle is flawed. As we previously submitted (CLPC IP 31, Submission 4-19.1) in relation to NPP 4.2, UPP 8.1(b) allows organisations to justify retention on the basis of the myriad secondary purposes for which NPP 2 allows the information to be potentially 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	(b) destroy or render non-identifiable personal information if it is no longer needed for a purpose for which it was collected and retention is not required by law. ALTERNATIVE WORDING (b) destroy or render non-identifiable personal information unless (i) there is an express legal requirement for its retention; or (ii) the agency or organisation has a reasonable expectation that it will use the information at a future date for the purpose for which it was collected.

	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 (p. 53, CLPC72). • We submit two alternative forms of words for a retention/disposal principle.	
	• The additional requirement of UPP 8.1(c) proposed in DP72 has been lost in Report 108 and should be reinstated. Clearly stating obligations of third party recipients is necessary to ensure that anyone who discloses personal information is obliged to take reasonable steps to ensure that it is protected against handling otherwise than in accordance with the UPPs. • It is not clear why the protection that the third party must provide was limited in the DP72 proposal 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 8.1(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) (p. 54, CLPC72). • Compliance with UPP 8.1(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?' in order to satisfy UPP 5, so it is little more of a burden to add 'and how will you comply with privacy principles?' (see pp. 54-55, CLPC72).	(c) ensure that personal information it discloses to a third person is protected in the possession of that person in accordance with all UPPs relevant tthat information.
	• There is a significant risk of misuse of security concerns by the over-zealous application of UPP 8.1(a) or (b), resulting in	8.2 For the purposes of this Principle, reasonable steps must be

	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 8.1(a)-(c) (see CLPC IP31, Submission 4-17) ((pp. 51-52, CLPC72).	proportional to the likelihood and severity of loss or damage to the indvidual and the sensitivity of the information.
8.2 The requirement to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act 1983* (Cth).	• We support the need for clarification of the relationship between a data disposal requirement in the UPPs and agencies retention obligations under the Archives Act. This provision is acceptable but needs to be supported by clear guidance, as recommended by the ALRC in Recommendation 28-5, but to be expressly agreed by the Privacy Commissioner and the National Archives.	8.3The requirement to destroy or render non-identifiable personal information is not 'required by law' for the purposes of the *Archives Act 1983* (Cth).
Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.	• We suppor the inclusion of this Note, subject to our submission below concerning data breach notification requirements.	Note: Agencies and organisations also should be aware of their obligations under the data breach notification provisions.

UPP 9. Access and Correction	*Comments*	*UPP 9. Access and Correction*
9.1 If an agency or 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:	• We make some comments below on the Access and Correction principle, but reserve the option of making further submissions on the complex interaction of privacy and FOI law, particularly in the context of the as yet uncertain government plans for FOI law reform.	9.1 If an agency or 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:
Where the information is held by an agency: (a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or		Where the information is held by an agency: (a) the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; or
Where the information is held by an organisation: (b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;	• In this instance we support the deletion of the word 'imminent' (p. 56, CLPC72).	Where the information is held by an organisation: (b) providing access would be reasonably likely to pose a serious threat to the life or health of any individual;
(c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;	• We support inclusion of these grounds for withholding, which are taken unchanged from NPP6, and do not appear to have caused any difficulty (p. 58, CLPC72).	(c) providing access would have an unreasonable impact upon the privacy of individuals other than the individual requesting access;
(d) the request for access is frivolous or vexatious;	• We support inclusion of these grounds for withholding, which are taken unchanged from NPP6, and do not appear to have caused any difficulty (p. 58, CLPC72).	(d) the request for access is frivolous or vexatious;
(e) 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	• We support inclusion of these grounds for withholding, which are taken unchanged from NPP6, and do not appear to have caused any difficulty (p. 58, CLPC72).	(e) 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

proceedings;		discovery in those proceedings;
(f) 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 (p. 56, CLPC72).	(f) 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. The extent of the refusal must be proportionate to the significance of the negotiations;
(g) providing access would be unlawful;	• We support inclusion of these grounds for withholding, which are taken unchanged from NPP6, and do not appear to have caused any difficulty (p. 58, CLPC72).	(g) providing access would be unlawful;
(h) denying access is required or authorised by or under law;	• Consistent with our submission onthe similar exception in UPP 5 (and elsewhere), we submit that this exception needs to be qualified – required or *specfically* authorised - (see p. 57, CLPC72). It is particularly important that this withholding ground be as limited as possible, given the history of self-serving interpretation of FOI laws to limit disclosure.	(h) denying access is required or specifically authorised by or under law;
(i) 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 (p. 58, CLPC72).	(i) providing access would be likely to prejudice an investigation of possible unlawful activity;
(j) 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; (ii) enforcement of laws relating to the confiscation of the proceeds of crime; (iii) protection of the public revenue; (iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; 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 (i) is available for internal investigations of suspected unlawful activity. (p. 57, CLPC72)	(j) 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; (ii) enforcement of laws relating to the confiscation of the proceeds of crime; (iii) protection of the public revenue; (iv) prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or (v) preparation for, or conduct of, proceedings before

(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	A Note should be inserted, with wording consistent with that of the Note in UPP 5.	any court or tribunal, or implementation of its orders; by or on behalf of an enforcement body; or Note: Exception (j) requires the active involvement, at an appropriate stage, of an Australian enforcement body.
(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.		(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.
9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.	• 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 – was addressed specifically in DP72, Proposal 55-3) and Proposal 7.5(d) addressed the issue of other types of information (such as unintelligible algorithms) which may also require special consideration when responding to access requests (p. 58, CLPC72). It is regrettable that in Report 108, the ALRC does not make any more specific recommendations , and in the case of credit scoring has taken a weaker position in response to industry lobbying.	9.2 Where providing access would reveal evaluative information generated within the agency or organisation in connection with a commercially sensitive decision-making process, the agency or organisation may give the individual an explanation for the commercially sensitive decision rather than direct access to the information.
Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2.	• We support this proposed note, which addresses concerns we raised in our earlier submission: (CLPC72 Submission DP72-89).	Note: The mere fact that some explanation may be necessary in order to understand information should not be taken as grounds for withholding information under UPP 9.2
9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.	• 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 (p. 59, CLPC72). In Report 108, the ALRC leave this as a discretionary function. We submit that the PC should be the 'default' intermediary, with an obligation to perform the role if the parties cannot agree on an alternative.	9.3 If an agency or organisation is not required to provide an individual with access to his or her personal information it must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary. In the absence of agreement, the Privacy Commissioner would be the intermediary.

9.4 If an organisation charges for providing access to personal information, those charges:	• We support the inclusion of UPP 9.4 but suggest that in addition some binding benchmarks be provided both on response times and on fees (p. 60, CLPC72). These benchmarks could be set ieither in Regulations or in Privacy Commissioner Rules, in either case subject to appropriate consultation standards (see our submission on the structure of regulation).	9.4 If an organisation charges for providing access to personal information, those charges:
(a) must not be excessive; and		(a) must not be excessive; and
(b) must not apply to lodging a request for access.		(b) must not apply to lodging a request for access.
Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.	• We support the continuation of the existing Privacy Act provision that prohibits agencies from charging for access.	Note: Agencies are not permitted to charge for providing access to personal information under UPP 9.4.
9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.		9.5 An agency or organisation must provide personal information in the manner requested by an individual, where reasonable and practicable.
9.6 If an agency or organisation holds personal information about an individual that is, with reference to a purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:	• We welcome the ALRC's proposed removal of the onus on the individual to 'establish' inaccuracy etc, which we suggested in our earlier submission (p. 60, CLPC72). • 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 8.1(b) above. (see also p. 60, CLPC72). • 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 (p.	9.6 If an agency or organisation holds personal information about an individual that is, with reference to the purpose for which it is held, misleading or not accurate, complete, up-to-date and relevant, the agency or organisation must take such steps, if any, as are reasonable to:

	61, CLPC72).	
(a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and		(a) correct the information so that it is accurate, complete, up-to-date, relevant and not misleading; and
(b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.	• We support this obligation. 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 in such circumstances is a requirement to notify the data subject, who can then choose whether they wish to exercise their right (under UPP9.6(b)) to have previous recipients notified. There would however need to be criteria for the type of 'correction' of a person's record which would trigger the requirement 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. (see our submission on this below).	(b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.
9.7 If an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant and:		9.7 If an individual and an agency or organisation disagree about whether personal information is, with reference to a purpose for which the information is held, misleading or not accurate, complete, up-to-date or relevant and,

(a) the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant; and		the individual asks the agency or organisation to associate with the information a statement claiming that the information is misleading or not accurate, complete, up-to-date or relevant;
(b) where the information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth;	• We question why this qualification is necessary. Whether or not an individual has pursued other adminstrative law remedies, and the outcome, should be irrelevant. In many cases it would satisfy the individual – but if not, why should the indvidual not still be able to require an annotation?	
the agency or organisation must take reasonable steps to do so.	• 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). (p. 62, CLPC72). ALRC Report 108 does not address this suggestion. • 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 (p. 62, CLPC72).	the agency or organisation must take reasonable steps to do so. Any annotation must be made available to any subsequent user of the disputed information.
9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:		9.8 Where an agency or organisation denies a request for access or refuses to correct personal information it must provide the individual with:
(a) reasons for the denial of access or refusal to correct the information, except to the extent that providing such reasons would undermine a lawful	• 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	(a) reasons for the denial of access or refusal to correct the information, specifying which of the exceptions in UPP 9 apply, except to the extent that providing such reasons would

reason for denying access or refusing to correct the information; and	the grounds specified at the time – it should not be open to an agency or organisation to later rely on alternative grounds (as happens all too often under FOI laws).	undermine a lawful reason for denying access or refusing to correct the information; and
(b) notice of potential avenues for complaint.		(b) notice of potential avenues for complaint.

UPP 10. Identifiers (only applicable to organisations)	***Comments***	***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:	• The principle should be applicable to agencies and organisations. We note that there is a precedent for this in the Victorian Information Privacy Act 2000 – IPP 7 (Unique Identifiers) is based on NPP 7 and applies to Victorian government agencies.	10.1 An agency or organisation must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:
(a) an agency;		(a) an agency;
(b) an agent of an agency acting in its capacity as agent;		(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		(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.		(d) an Australian state or territory agency.
	• In accordance with the underlying 'proportionality' principle, this Principle should limit the assignment of identifiers in the first place. There is a precedent for this in the NSW Health Records and Information Privacy Act 2002 - HPP 12(1) which provides that a public or private sector 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". The efficiency qualification is in our view redundant as it is implicit in the 'reasonably necessary' test, which is used throughout the principles. This requirement could of course only apply to Commonwealth agencies – although we would hope that State and Territory legislation would apply this 'purpose justification' requirement to their own agencies.	10.2 An agency may only assign identifiers to individuals if the assignment of identifiers is reasonably necessary to enable the agency to carry out any of its functions.

10.2 Where an identifier has been 'assigned' within the meaning of UPP 10.1 an organisation must not use or disclose the identifier unless:		10.~~2~~3 Where an identifier has been 'assigned' within the meaning of UPP 10.1 an agency or organisation must not use or disclose the identifier unless:
(a) the use or disclosure is necessary for the organisation to fulfil its obligations to the agency that assigned the identifier;		(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; or		(b) one or more of UPP 5.1(c) to (f) apply to the use or disclosure; or
(c) the identifier is genetic information and the use or disclosure would be permitted by the new *Privacy (Health Information) Regulations*.	• our general comments about procedural safeguards for the making of Regulations are relevant.	(c) the identifier is genetic information and the use or disclosure would be permitted by the new *Privacy (Health Information) Regulations*.
10.3 UPP 10.1 and 10.2 do not apply to the adoption, use or disclosure by a prescribed organisation of a prescribed identifier in prescribed circumstances, set out in regulations made after the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.	• 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 (p. 65, CLPC72). • If it is decided to provide for exceptions in Regulations, our general comments about procedural safeguards for the making of Regulations are relevant.	
10.4 The term 'identifier', for the purposes of UPP 10, includes a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification 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 (p. 65, CLPC72). • There is no justification for limiting this provision to 'automated biometric' identification or verification. It should apply to any identification or verification using the number etc.	10.4 The term 'identifier', for the purposes of UPP 10, includes a number, symbol, biometric information or other particular that is
(a) uniquely identifies or verifies the identity of an		(a) collected for the purpose of uniquely identifiyinges or

individual for the purpose of an agency's operations; or		verifying~~ies~~ the identity of an individual for the purpose of an agency or organisation's operations; or
(b) is determined to be an identifier by the Privacy Commissioner.		(b) determined to be an identifier by the Privacy Commissioner.
However, an individual's name or ABN, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.	• We can see no justification for excluding the ABN from this Principle – its legitimate use is accommodated by the Principle in the same way as for TFNs	
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).		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).

UPP 11. Cross-border Data Flows	*Comments*	*UPP 11. Cross-border Data Flows*
11.1 If an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, the agency or organisation remains accountable for that personal information, unless the:	• The ALRC's 'accountability' approach would result in most transfers carrying no privacy protection once personal information had been transferred – almost all agencies or organisations would be able to take advantage of one of the exceptions in UPP11.1. We submit an alternative Principle which is a modification of the current 'border control' approach, but which also incorporates continued accountability in many cases. • Allowing transfers solely on the basis of 'accountability' of the recipient is an undesirable starting point, and extremely dangerous to the privacy of Australians. • Except where the transfer is required by Australian law, or on the basis of fully informed consent, the transferor should remain 'accountable' for any subsequently occurring breaches for which they could reasonably be expected to be liable. • However, transfers should not be allowed in any other circumstances (than those two) to jurisdictions which do not provide a level of protection substantially similar to that applying in Australia.. • 'Transfer' should include where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia. (p. 69, CLPC72). • 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 (p. 69, CLPC72). • There is no justification for limiting the application of UPP 11 to agencies or organisations ' in Australia or an external territory'. All of the UPPs should apply equally to all agencies and organisations wherever they are located – subject to the general jurisdictional limitations provided in section 5B (extra-territorial operation of the Act).	11.1 An agency or organisation shall not transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia and an external territory, unless :

(a) agency or organisation reasonably believes 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 these principles;	• There is no justification for the 'reasonable belief' qualification in this exception. The judgement as to whether a law provides 'substantially similar' protection should remain objective; i.e. it must be evidence-based. It is implicit that agencies and organisations are not expected to make unreasonable enquiries, but making this qualification express would provide too much room for self-serving assessments without adequate consideration. • The exception needs to cater for laws etc in other jurisdictions which may not be 'substantially similar' to the Australian Act but which may nonetheless offer better protection; e.g. by taking an alternative approach. • Agencies and organisations making transfers under this exception would remain accountable for compliance with all of the UPPs to the extent that it was reasonable to expect them to. • We support the ALRC's recommendation (31-7) for the Privacy Commissioner to publish guidance on appropriate clauses for contracts which could satisfy this exception.	(a) the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to, or or more favourable to data subjects than, this Act and which are enforceable by the subject of the personal information, or
(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or	• Transfers without continued accountability of the transferor may occur with the consent of the indivdual (s) concerned but only if the data subject is made specifically aware of every relevant aspect of the transfer that applies in their case. • We accept that in some circumstances for which this exception will appy, it is unreasonable to expect the transferring organisation to know much if anything about the intended uses, protections etc in the destination jurisdiction. For this reasons, some of the matters will only be required to be advised 'if known'. • We remain concerned about the potential for consent exceptions to be abused by 'bundling' but this is a generic issue that needs to be addressed in relation to the Act as a whole, rather than in specific principles or exceptions – see our separate submission on key concepts.	(b) the individual consents to the transfer, after being expressly advised of the country or countries which are the destination of the transfer, the intended recipient or recipients, and, if known, the intended uses, the protective measures (if any) that will be taken in relation to their information (or that there are none); and whether the personal information will be transferred from the destination country. The individual must also be expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or
(c) agency or organisation is required or authorised by or under law to transfer the personal information.	• Transfers without continued accountability of the transferor may occur where the transferor is required by Australian law to undertake the transfer, but not where they have an option whether or not to do so (I.e. merely authorised) and not	(c) the agency or organisation is required by Australian law to transfer the personal information, or

	where they are 'required' by some foreign law. If a transfer is required by a foreign law (and there is no conflict with other Australian law) and if a discretionary transfer is made where 'authorised" by an Australian law, the agency or organisation will remain accountable.	
	• The existing exception for transfers in the interests of the individual but where consent is impracticable (NPP9(e)) should also be included in the UPP. • Agencies or organisations making transfers under this exception will remain accountable for compliance with all of the UPPs to the extent that it was reasonable to expect them to. (see proposed UPP 11.3)	(d) All of the following apply: (i) the transfer is for the benefit of the individual; (ii) it is impracticable to obtain the consent of the individual to that transfer; (iii) if it were practicable to obtain such consent, the individual would be likely to give it.
	• The preferred means of satisfying the 'substantially similar' test in UPP 11.1(a) will be by reference to a whitelist instrument. Any 'whitelist' in relation to UPP 11.1(a) could be by a regulation or other legislative instrument made by the government (ALRC Report 108 Recommendation 31-6), but if so only after receipt of published advice from the Privacy Commissioner (p. 71, CLPC72)., which in turn should only be given after public hearings. Alternatively, and preferably, the instrument could be a determination by the Privacy Commissioner, after public hearings. • In order to qualify for the 'whitelist' for the purposes of UPP 11.1(a), a foreign jurisdiction must have in place an agreement on cross border enforcement with the Australian Privacy Commissioner (p. 71, CLPC72). • Inclusion on a whitelist will not be the only means of satisfying the 'substantially similar' test in 11.1(a), partly because it would take time for the Commissioner to assess foreign schemes., but also because it is envisaged that contractual arrangements may suffice. • In the absence of inclusion in a whitelist, an agency or organisation could make its own judgement that a law, binding scheme or contract met this test, but would have to be prepared to justify that judgement.	11.2 The Privacy Commissioner may make a determination that a recipient or a class of recipients of personal information satisfies the requirements of 11.1(a). The Privacy Commissioner shall hold public hearings before making a determination under this provision. A determination made under this provision is a legislative instrument. The Privacy Commissioner shall not make a determination under this provision unless there exists an agreement on cross border enforcement between the Privacy Commissioner and a relevant public authority responsible for data protection in the jurisdiction to which it is proposed to transfer the personal information.

	• Whether our alternative Principle is adopted, or (contrary to our submission) the ALRC's 'Accountability' approach is adopted, allowing for transfers even where none of the conditions in 11.1 are met, a definition of 'accountability' must be added - accountability' is meaningless in the current proposals . • The definition should seek to overcome the near impossibility of an ordinary person proving that an unknown organisation in a foreign country (probably one with no data protection authority, or (a) would apply) has breached a UPP. • The evidentiary burden should shift to the party that exports the personal information to a country that has no data protection laws equivalent to Australian laws. It should be up to them to prove, on the balance of probabilities, that any damage suffered by the person which might reasonably be assumed to be as a result of the breach of the UPPs by some overseas party has in fact arisen from some other cause. A legal presumption is the normal way to achieve such a result. Anything less is manifestly unfair.	11.3 The meaning of an agency or organisation remaining accountable under clause 11.1 is that: (a) Where personal information has been transferred pursuant to clause 11.1(a) or (d), and the person who is the subject of the personal information has suffered damage which it is reasonable to assume may have resulted from a breach of these Principles, then it is presumed that the damage did result from a breach of the Principles by the recipient of the information or by any person to whom the recipient of the information transferred the information either directly or indirectly. (b) Unless the agency or organisation can establish, on the balance of probabilities, that the damage has some other cause, it will be liable for a breach of the Principle or Principles which it is reasonable to assume have been breached by the recipient of the information or by any person to whom the recipient of the information transferred the information either directly or indirectly.
	• Because cross border transfers of personal information will always involve an element of risk, we submit that individuals are entitled to be expressly informed of proposed transfers, so that they can either challenge the practice, or take their transactions elsewhere if they remain unhappy about the proposed destination. • We have already suggested a notice condition to 'consent' exception. This proposed sub-principle provides for notice where transfers are made under the other three exceptions.	[Proposed clause to deal with provision of notice: 11.4 At or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation transfers personal information in accordance with 11.1(a) (c) or (d), the agency or organisation must give the individual notice of (i) the jurisdiction in which the recipient is located; (ii) the identity of the recipient; (iii) functional contact details of the recipient; and (iv) under which provision the information is transferred.
	• We submit that this Principle should also apply 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 agency or organisation 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? (p. 70, CLPC72). The ALRC's	[Proposed clause to deal with inter-Australian transfers: 11.5 This Principle applies to transfers of personal information about an individual to a government of a jurisdiction within Australia insofar as the meaning of the Principle allows.

	formulation does not allow for modification to achieve this result, but there should be a separate clause which does so (see proposed clause 11.5).	
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 Australia.		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 Australia.

Data breach notification	***Comments***	***UPP x. Data Breach Notification (or a sub-part of UPP 8)***
The ALRC recommends a data breach notification requirement, but in a separate part of the Act, not in a UPP. (DP72, Chapter 47 and Proposal 47-1)	• We support the general thrust of the ALRC's proposals concerning data breach notification but are addressing the matter here because we consider that there is a good case to be made for including the requirement in the UPPs either as an additional UPP 12, or alternatively part of UPP 8 (Security) (since it is a requirement that is consequential to a security breach). • Procedural provisions related to the requirement could go elsewhere in the Act, but the basic 'high level' principle should in our view be found in the UPPs. • Unless the data breach notification requirement is a UPP it will not be enforceable through individual complaints, but only enforceable by the Commissioner through an 'own motion' investigation and notice, with a civil penalty sanction for non-compliance. While these options are valuable, we submit that allowing individuals to directly challenge a failure to notify would lead to much higher levels of compliance with the requirement, which may otherwise be largely ignored, on a rational risk management calculation • Making the data breach notification requirement a UPP would also make it more likely that such a requirement 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(p. 80, CLPC72). • As part of the UPPs, a data breach notification requirement would be included in the first stage of the government's legislative response, rather than left to the as yet unscheduled second stage. We can see no good arguments for delaying introduction of this requirement, which is rapidly becoming a standard tool in other jurisdictions, and is 'expected' by most internationally aware organisations. • The ALRC' data breach disclosure requirement is incoherent and circular. It allows avoidance of disclosure of breaches, even to the Privacy Commissioner, on the basis of subjective judgments by the party in breach.	Proposed principle (UPP x or a new part of UPP 8:) x.1 An agency or organisation must notify the Privacy Commissioner when personal information has been exposed to unauthorised persons, and there is a reasonable likelihood of significant loss or damage to one or more individual. x.2 In cases subject to x.1, the agency or organisation must notify individuals whose information may have been exposed within 24 hours Procedural provisions which could either go in the Principle or elsewhere in the Act: • On becoming aware of a security breach which may involve the disclosure of personal information, an agency or organisation must consider if (a) there is a reasonable likelihood that personal information has been exposed to unauthorised persons and (b) there is a reasonable likelihood of signficant loss or damage to one or more individual. • If the breach meets these two conditions, the agency or organisation must first notify Privacy Commissioner, and then notify affected individuals unless the Privacy Commissioner advises (on request or otherwise) that notification of individuals is not appropriate in the circumstances. • Agencies and organisations must keep a register of breaches, with details of the assessment of exposure risk and likelihood of loss or damage. The register would be available to the Privacy Commissioner at any time on request, and a regularly updated summary of the number and type of incidents to be publicly available on request, and published at least annually in a readily accessible form (e.g. Annual Report).

	• We propose a revised data breach notification requirement. We put it forward here as a UPP, but it could as a 'second best' equally be in a separate part of the Act, although in this case we submit it should be brought forward into the first stage legislative amendments. • The concept of 'specified' personal information' is redundant – *any* information may give rise to a risk of loss or damage , depending on the context – this is taken into account in the assessment of likelihood of significant loss or damage • 'loss or damage' is preferable to 'harm' as the former expression is already used in Part V of the Act (where it is defined to include injury to feelings or humiliation – an important inclusion, with the safeguard of the 'significant' qualifier. • 'significant' is preferable to 'serious' as a test in the assessment to trigger notification. • 'exposure to unauthorised persons' is preferable to 'acquired by an unauthorised person' – in many data breach scenarios it may be impossible to ascertain if information has actually been acquired – it is much more likely to be clea r whether or not the information has been exposed. • Placing the requirement in a UPP effectively reverses the onus - if challenged by an individual complaint, an agency or organisations would have to justify why it considered the breach did not give rise to a reasonable likelihood of significant loss or damage. This is far preferable to the ALRC proposal for the agency or organisation to be the sole judge of whether there was a risk of serious harm – the only 'check' being the unlikely prospect of an audit, inspection or own-motion investigation by the Privacy Commissioner.	• The Privacy Commissioner should issue guidelines to address matters to be taken into account in making the assessment of the need to notify; e.g. adequate encryption may have prevented exposure, and the nature of the information may mean a low likelihood of significant loss or damage. • Failure to notify the Commissioner of breaches meeting the criteria, to keep an adequate register, or to respond to public requests for summaries of breach history (in common with other non-compliance with the UPPs) should attract a civil penalty if these failures were serious or repeated).

No disadvantage	*Comments*	*UPP y. 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 is already incorporated in some of the existing principles and would be incorporated where practicable the UPPs or other provisions (Report 108, 32.29-32.34). • We doubt that such measures can adequately substitute for a separate principle as in the Australian Privacy Charter and the Asia Pacific Privacy Charter) (p. 82, CLPC72). • 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 (p. 82, CLPC72).	y.1 Individuals should not be denied goods or services or offered them on unreasonably disadvantageous terms (including higher cost) in order to enjoy the rights conferred by the UPPs.
Enforcement		
The ALRC recommends a strengthening of the enforcement regime under the Act, to include a power for the Commissioner to issue 'compliance notices' both in complaint determinations and following own-motion investigations (Report 108 Recommendation 50-1), and civil penalties for serious or repeated breaches of the UPPs, and and enforceable undertakings (Recommendations 50-2 & 50-4).	• We strongly support these proposals, as essential to give more 'teeth' to the Act and fill in the existing gaps in the enforcement pyramid. • They will however only be effective to the extent that the powers are used by the incumbent Privacy Commissioner, and we submit that the appointment of a Commissioner willing to take a proactive approach to enforcement is at least as important as the legislative amendments.	