Australian Privacy Foundation
post: GPO Box 1196
Sydney NSW 2001
email: mail@privacy.org.au
web: www.privacy.org.au

Review of Australian Privacy Law
Discussion Paper 72
September 2007
Australian Privacy Foundation
Submission to the Australian Law Reform Commission
December 2007

Contents

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the leading non-governmental organisation dedicated to protecting the privacy rights of Australians. We aim to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

Since 1987 the Australian Privacy Foundation has led the defence of the rights of individuals to control their personal information and to be free of excessive intrusions. We use the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed.

For further information about the organisation, see www.privacy.org.au

Introduction

We congratulate the ALRC on a very thorough consideration of issues and what we regard as a generally progressive set of proposals which will both strengthen and simplify privacy protection in Australia. Individuals, government agencies and private sector organisations would all benefit from the adoption of the proposals, which we hope will be reflected in the Commission's final recommendations, subject to various qualifications and reservations in this submission.

Changed political environment

We note that the ALP made certain commitments in its election platform concerning Privacy and Freedom of Information law. The new federal Government has moved quickly to announce some changed administrative arrangements, including transfer of administrative responsibility for both Acts from the Attorney-General's Department to the Department of Prime Minister and Cabinet, under the direction of the Special Minister of State.

We believe the ALRC needs to respond to this changed political environment. Following the planned course of the review and only reporting in March 2008 would in our view risk 'missing the boat' if the government is determined to take early action on some privacy and FOI reforms, including implementing the Commission's 1995 recommendations in its 'Open Government' report (ALRC 77). We suggest that the ALRC identifies those of its proposals which can stand alone and for which there is broad support, and takes an early opportunity to brief the government on a set of recommendations for early implementation. Those other proposals which involve more complex interactions, require further discussion or are particularly controversial can be delivered to the government on the original, or somewhat relaxed, timetable.

We also note that the new government may be considering the adoption of a statutory charter of human rights. This would alter the context of privacy law by providing a complementary means of promoting the right to privacy, which would be included in any Charter based on the Universal Declaration of Human Rights (Article 8) or the International Covenant on Civil and Political Rights (Article 17). The ALRC should take this new development into account in its final report.

Regulatory hierarchy

Whilst not clearly spelt out in DP72, it appears that the ALRC envisages a hierarchy of regulation with a number of 'tiers':

- The Privacy Act, including Unified Privacy Principles (UPPs)
- Regulations – special rules at least for Health Information and Credit Reporting
- Binding Rules issued by the Privacy Commissioner under the Privacy or other Acts, including replacements for some of the current 'Guidelines' – e.g. TFN, NH&MRC, Medicare and Pharmaceutical Benefits Programs, and Data-matching Program.
- Binding Codes, issued or approved by the Privacy Commissioner under Part IIIAA.
- Public Interest Determinations, made by the Privacy Commissioner under Part VI (allowing waivers from the UPPs in specific circumstances).
- Advisory Codes
- Advisory OPC Guidance (Guidelines)

While we can understand the reasoning behind the ALRC's proposals for each of these levels, it is arguable whether the proposed hierarchy, overall, meets the objective of a simplified regime. It should be possible to achieve some further rationalisation.

Varying the Principles

It appears that Regulations and binding Rules could vary the standards required both upwards and downwards from the 'baseline' UPPs, while binding Codes could only impose obligations that, overall, are at least the equivalent of those in the UPPs. Public Interest Determinations would only be made to vary the standards downwards.

Binding rules or Codes would continue to be legislative instruments subject to disallowance by Parliament, but in our view, this is a lesser safeguard than is often assumed – governments typically face less scrutiny over, and find it much easier to push through, other disallowable instruments than legislative amendments or Regulations.

Assuming that there will be a hierarchy of instruments, our overall position is that more of the detail needs to be in either the Act or Regulations, rather than being left to the instruments developed by the Privacy Commissioner. This is based on a limited confidence in OPC's capability and commitment. This is admittedly founded on historical experience (of the last 18 years), and the reforms to the role of the Commissioner which the ALRC proposes in Part F of DP72 will hopefully allow more confidence in future, but until this is demonstrated, we favour more of the key privacy protection provisions being embedded in the Act or Regulations.

We also have some reservations about the value of OPC advisory guidance, based on its limited status in any litigation[1], and experience to date. Also, advisory guidance will only be of an adequate standard, and carry credibility, if it results from a properly resourced and conducted consultation process involving all relevant stakeholders. Experience of the APF since the commencement of the Privacy Act in 1989 is that consultation processes are often inadequate. Even when adequate on their face they often result in unbalanced and unsatisfactory outcomes due to unequal input and influence as between different classes of stakeholder – most often the ability of business interests to resource a much higher and sustained level of input than civil society NGOs.

This reservation applies equally to the development of any binding Codes or Rules for which the Commissioner is responsible.

Statutory timelines

Another general submission is that where timelines are involved e.g. for responding to access requests or opt-outs, specific periods should be included in the Act or Regulations rather than being left to Codes or guidance. There are plenty of precedents for response times being legislated, both in administrative law and business regulation.

Structure of submission

Several of our members have contributed to our review of DP72. It proved impossible, given our all-volunteer resources, to complete the submission before Xmas – already two weeks after the ALRC's formal submission deadline. In order to prevent any further delay, we have not consolidated the submission into a common format. Our submissions on Parts A-G of DP72 are presented in tables, while our submissions on Chapter 58 (Research) and Part I (Children, Young People and Adults requiring assistance), together with a supplementary submission on biometric technology in Part B are in a document form. We acknowledge the assistance of the Office of the Privacy Commissioner (OPC) and the Public Interest Advocacy Centre (PIAC) who provided the template of the tables of ALRC proposals use in our response to Parts A-G.

Our submissions on Chapters 56 & 57 (Health services) and Part J (Telecommunications) are not yet complete and will follow as soon as practicable. We will also be making a more detailed submission on the proposed private right of action (Chapter 5).

[1] See Nicholson, J, in ACMA v Clarity 1 Pty Ltd (2006) 150 FCR 494 (referenced in DP72 paragraph 64.77)

Please note that postal correspondence takes some time due to re-direction – our preferred mode of communication is by email to mail@privacy.org.au, which should be answered without undue delay.

DP72 Part A – Introduction

ALRC PROPOSALS	APF SUBMISSION
PART A Introduction	
Ch 1 – Introduction to the Inquiry	
Proposal 1–1 The Office of the Privacy Commissioner should, either on its own motion or where approached in appropriate cases, encourage and assist agencies and organisations, in conjunction with Indigenous and other ethnic groups in Australia, to create publicly available protocols that adequately respond to the particular privacy needs of those groups	We support Proposal 1-1 in principle but it must be clearly limited to avoid an argument in favour of ''corporate' privacy. Legal entities should not have rights under Information privacy legislation
Ch 2 – Privacy Regulation in Australia	
No proposals.	
Ch 3 – The Privacy Act 1988 (Cth)	
Proposal 3–1 The *Privacy Act* should provide that the Governor-General may make regulations that modify the operation of the proposed Unified Privacy Principles (UPPs) to impose different or more specific requirements in particular contexts, including imposing more or less stringent requirements on agencies and organisations than are provided for in the UPPs.	We support Proposal 3-1 in principle but are concerned about providing for Regulations that allow LESS stringent requirements. The credit reporting requirements in Part IIIA are mostly more stringent (see our submission on Part G) but we concede that there may be a need for some less stringent requirements in particular contexts, such as in Health Services (see our submission on Part I). We refer to the Introduction to our submission in which we stress the importance of any 'derogation' from the UPP standards being positively affirmed *by* Parliament rather than left to the discretion of the Privacy Commissioner, even if the latter instruments are subject to disallowance.
Proposal 3–2 The *Privacy Act* should be amended to achieve greater logical consistency, simplicity and clarity. For example, the IPPs and the NPPs should be consolidated into the Unified Privacy Principles (UPPs), the exemptions should be clarified and grouped together in a	Support

ALRC PROPOSALS	APF SUBMISSION
separate part of the Act and the Act should be restructured and renumbered.	
Proposal 3–3 If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, the name of the Act should remain the same. If the Act is not amended in this way, however, the *Privacy Act* should be renamed the *Privacy and Personal Information Act*.	Support
Embedded position: Name of Act: The ALRC does not agree that the Act should be renamed the Australian Privacy Act. 'Australian' is often included in the title of legislation at the national level where it forms part of the name of the organisation established by the legislation, for example, *Australian Law Reform Commission Act 1996* (Cth).	
Proposal 3–4 The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be to:	We support an objects clause but as proposed this is a collection of disparate objectives or caveats, not all of equal 'weight'
(a) implement Australia's obligations at international law in relation to privacy;	
(b) promote the protection of individual privacy;	This should be elevated to the primary object, with others as subordinate objectives or qualifiers
(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance the public interest in protecting the privacy of individuals with other public interests;	
(d) establish a cause of action to protect the interests that individuals have in the personal sphere free from interference from others;	
(e) promote the responsible and transparent handling of personal information by agencies and organisations;	
(f) facilitate the growth and development of electronic commerce, nationally and internationally, while ensuring respect for the right to privacy; and	
(g) provide the basis for nationally consistent regulation of privacy.	
Proposal 3–5 (a) The *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.	We agree that there needs to be a second leg to the definition, as much personal information will be held in a form that is not identified on its face. However, we submit that the qualifier should be 'potentially' rather than 'reasonably' to catch all those situations

ALRC PROPOSALS	APF SUBMISSION
	where components are initially separate but can be brought together to form an effective identifier. 'Reasonably' is too narrow to cover all such situations.
(b) The Explanatory Memorandum of the amending legislation should make clear that an individual is 'reasonably identifiable' when the individual can be identified from information in the possession of an agency or organisation or from that information and other information the agency or organisation has the capacity to access or is likely to access.	This is such a significant definition that all aspects of it must, in our view, be in the Act itself. See also our submission on proposal 3.5(a)
(c) The Office of the Privacy Commissioner should provide guidance on the meaning of 'identified or reasonably identifiable'.	Support, but see our submissions about the restricted status of OPC guidance (see our submissions Introduction and on Part F (Proposal 44-2)
Embedded Position: **Definition of Personal Information:** 'In the ALRC's view, information that simply allows an individual to be contacted—such as a phone number, a street address or an IP address—in isolation, would not fall within the proposed definition of 'personal information'. *The Privacy Act is not intended to implement an unqualified 'right to be let alone'*. (para 3.139 – emphasis added)	These would almost certainly be caught in most cases because other information allowing identification would be available
Proposal 3–6 The definition of 'sensitive information' in the *Privacy Act* should be amended to include: (a) biometric information collected for the purpose of automated biometric authentication or identification; and (b) biometric template information.	Support
Proposal 3–7 The definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual preferences and practices'.	Support
Embedded Position: Financial Information: The ALRC's view is that financial information should not be included in the definition of sensitive information in the *Privacy Act*. (para 3.168)	Support
Proposal 3–8 The definition of 'record' in the *Privacy Act* should be amended in part to include: (a) a document; and (b) information stored in electronic or other forms.	Support
Embedded position: Photographs: The ALRC agrees that photographs or other pictorial representations should be covered by the term 'record' in the *Privacy Act* and that they should not be limited by the phrase 'of a person'. This can be achieved by relying on the definition of	Support

ALRC PROPOSALS	APF SUBMISSION
'document' in the *Acts Interpretation Act*, which includes 'any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device'. (at para 3-185)	
Embedded position: Definition of Record: The ALRC does not agree that the definition of record needs to 'stand alone.'… The term 'record' is defined in the *Acts Interpretation Act*. It includes 'information stored or recorded by means of a computer'. The ALRC's view is that this definition is not sufficient in the context of the *Privacy Act.* (para 3.182 – 3.183).	Support
Proposal 3–9 The definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.	Support
Proposal 3–10 The personal information of deceased individuals held by agencies should continue to be regulated by the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth).	Support
Proposal 3–11 The *Privacy Act* should be amended to include a new Part dealing with the personal information of individuals who have been dead for 30 years or less where the information is held by an organisation. The new Part should provide as follows:	Support
(a) Use and disclosure Organisations should be required to use or disclose the personal information of deceased individuals in accordance with the proposed 'Use and Disclosure' principle in the UPPs. Where the principle requires consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.	Support
(b) Access Organisations should be required to consider providing third parties with access to the personal information of deceased individuals in accordance with the access elements of the proposed 'Access and Correction' principle in the UPPs. Organisations should be required to consider in each case whether providing access to the information would have an unreasonable impact on the privacy of other individuals, including the deceased individual.	Support

ALRC PROPOSALS	APF SUBMISSION
(c) Data quality Organisations should be required to ensure that the personal information of deceased individuals is, with reference to a use or disclosure permitted under the UPPs, accurate, complete, up-to-date and relevant before they use or disclose the information.	Support
(d) Data security Organisations should be required to take reasonable steps to protect the personal information of deceased individuals from misuse and loss and from unauthorised access, modification or disclosure. Organisations should be required to take reasonable steps to destroy or render personal information of deceased individuals non-identifiable if it is no longer needed for any purpose permitted under the proposed UPPs.	Support
Organisations should be required to take reasonable steps to ensure that personal information of deceased individuals they disclose to a person pursuant to contract, or otherwise in connection with the provision of a service, is protected from being used or disclosed by that person otherwise than in accordance with the *Privacy Act*.	Support
Proposal 3–12 The proposed provisions dealing with the use or disclosure of personal information of deceased individuals should make clear that it is reasonable for an organisation to use or disclose genetic information to a genetic relative of a deceased individual where the organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. Any use or disclosure of genetic information of deceased individuals should be in accordance with rules issued by the Privacy Commissioner.	Support (it *is* appropriate not to include the qualifier 'imminent' here, unlike in some of the UPPs – see our submission on Part D)
Proposal 3–13 Breach of the proposed provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner alleging an interference with the privacy of a deceased individual: (a) in relation to an alleged breach of the use and disclosure, data quality or data security provisions, the deceased individual's parent, child or sibling who is at least 18 years old, spouse, de facto partner or legal personal representative; and (b) in relation to an alleged breach of the access provision, any person who has made a request	Support

ALRC PROPOSALS	APF SUBMISSION
for access to the personal information of a deceased individual.	
Ch 4– Achieving National Consistency	
Proposal 4–1 The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations: (a) *Health Records and Information Privacy Act 2002*(NSW); (b) *Health Records Act 2001* (Vic); (c) *Health Records (privacy and Access Act 1997* (ACT); and (d) any other laws prescribed in the regulations.	Support
Proposal 4-2 States and territories with information privacy legislation that purports to apply to private sector organisations should amend that legislation so that it is no longer expressed to apply to private sector organisations.	Support
Proposal 4-3 The Privacy Act should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'non-excluded matters' set out in the legislation. The Australian Government, in consultation with state and territory governments should develop a list of 'non-excluded matters', for example matters such as: (a) reporting for child protection purposes; (b) reporting for public health purposes; and (c) the handling of personal information by state and territory government contractors.	Support
Proposal 4–4 The states and territories should enact legislation that regulates the handling of personal information in that state or territory's public sector that: (a) applies the proposed Unified Privacy principles and the proposed Privacy (Health Information) Regulations as in force under the *Privacy Act* from time to time; and (b) include at a minimum: (i) relevant definitions used in the *Privacy Act* (including 'personal information',	Support – we would like to see the ALRC canvass the options in more detail e.g. uniform or model laws – see our submission on Proposal 4-6

ALRC PROPOSALS	APF SUBMISSION
'sensitive information' and health information); (ii) provisions allowing public interest determinations and temporary public interest determinations; (iii) provisions relating to state and territory incorporated bodies (including statutory corporations); (iv) provisions relating to state and territory government contracts; and (v) provisions relating to data breach notification. The legislation should also provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.	
Proposal 4-5 The Australian Government should initiate a review in five years to consider whether the proposed Commonwealth-state cooperative scheme has been effective in achieving national consistency. This review should consider wither it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors.	Support
Proposal 4-6 To promote and maintain uniformity, the Standing Committee of Attorney-General (SCAG) should adopt an intergovernmental agreement which provides that any proposed changes to the proposed: (a) Unified Privacy Principles must be approved by SCAG; and (b) Privacy (Health Information) Regulations must be approved by SCAG, in consultation with the Australian Health Ministers' Advisory Council (AHMAC). The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be consider and approved by SCAG before being implemented.	We would like to see more detailed options e.g. model or uniform laws We have reservations, based on experience, about how well or quickly SCAG works
Proposal 4–7 The Standing Committee of Attorneys-General (SCAG) should be assisted by an expert advisory committee to: (a) provide advice in relation to the amendment of the proposed Unified Privacy Principles and the proposed *Privacy (Health Information) Regulations*;	Support – subject to our reservations about SCAG

ALRC PROPOSALS	APF SUBMISSION
(b) address issues related to national consistency such as the scrutiny of federal, state and territory bills that may adversely impact on national consistency in the regulation of personal information; and (c) address issues related to the enforcement of privacy laws, including information sharing between privacy regulators and cooperative arrangements for enforcement. Appointments to the expert advisory committee should ensure a balanced and broad-based range of expertise, experience and perspectives relevant to the regulation of personal information. The appointments process should involve consultation with state and territory governments, business, privacy and consumer advocates and other stakeholders.	
Ch 5 – Protection of a Right to Personal Privacy	
Proposal 5–1 The Privacy Act should be amended to provide for a statutory clause of action for invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall with the cause of action. For example, an invasion of privacy may occur where: (a) there has been an interference with an individual's home or family life; (b) an individual has been subjected to unauthorised surveillance; (c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; (d) sensitive facts relating to an individual's private life have been disclosed.	Support in principle – detailed comment to follow in a separate submission
Proposal 5–2 The *Privacy Act* should provide that, in determining what is considered 'private' for the purposes of establishing liability under the proposed statutory cause of action, a plaintiff must show that in all the circumstances: (a) there is a reasonable expectation of privacy; and (b) the act complained of is sufficiently serious to cause substantial offence to a person of ordinary sensibilities.	We support this proposal, but it would need re-wording to relate to all grounds in Proposal 5-1, as the word 'private' is only used in grounds (c) and (d)
Proposal 5–3 the *Privacy Act* should provide that: (a) only natural persons should be allowed to bring an action under the *Privacy Act* for invasion of privacy;	Support in principle – detailed comment to follow in a separate submission

ALRC PROPOSALS	APF SUBMISSION
(b) the action is actionably without proof of damage; and (c) the action is restricted to intentional or reckless acts on the part of the defendant.	
Proposal 5–4 The Office of the Privacy Commissioner should provide information to the public concerning the proposed statutory cause of action for invasion of privacy	Support in principle – detailed comment to follow in a separate submission
Proposal 5–5 The range of defences to the proposed statutory cause of action for invasion of privacy provided for in the Privacy Act should be listed exhaustively. That list should include that the: (a) act or conduct was incidental to the exercise of a lawful right of defence of person or property; (b) act or conduct was required or specifically authorised by or under law; (c) information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or (d) disclosure of the information was, under the law of defamation, privileged.	Detailed submission to follow
Question 5–1 In addition to the defences listed in Proposal 5-5, are there any other defences that should apply to the proposed statutory cause of action for invasion of privacy?	Detailed submission to follow
Proposal 5–6 To address an invasion of privacy, the court should be empowered by the *Privacy Act* to choose the remedy that is most appropriate in all the circumstances, free from the jurisdictional constraints that may apply to that remedy in the general law. For example, the court should be empowered to grant any one or more of the following: (a) damages, including aggravated damages, but not exemplary damages; (b) an account of profits; (c) an injunction; (d) an order requiring the defendant to apologise to the plaintiff; (e) a correction order; (f) an order for the delivery up and destruction of material;	Support in principle – detailed comment to follow in a separate submission

ALRC PROPOSALS	APF SUBMISSION
(g) a declaration; and (h) other remedies or orders that the court thinks appropriate in the circumstances	
Proposal 5– 7 Until such time as the states and territories enact uniform legislation, the state and territory public sectors should be subjected to the proposed statutory cause of action for invasion of privacy in the *Privacy Act.*	Support in principle – detailed comment to follow in a separate submission

DP72 Part B – Developing Technology

ALRC PROPOSALS	APF SUBMISSION
PART B – Developing Technology	
Ch 6 – Impact of Developing Technology on Privacy	
Invitation for further comment [6.97] – The ALRC is interested in hearing about other technologies that may impact on privacy.	Our separate submission on Biometric Technologies appears after this table.
Ch 7 – **Accommodating Developing Technology in a Regulatory Framework**	
Proposal 7–1 The *Privacy Act* should be technologically neutral.	Support but add 'The overall privacy protection framework should be designed so as to ensure ongoing awareness of the impacts of technology, and to avoid blindness to them.'
Proposal 7–2 The *Privacy Act* should be amended to empower the Minister responsible for the *Privacy Act*, in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.	Support, subject to reservations about standards processes
Proposal 7–3 In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy enhancing way by individuals, agencies and organisations.	Support
Proposal 7–4 The Office of the Privacy Commissioner should educate individuals, agencies and organisations about specific privacy enhancing technologies and the privacy enhancing ways in which technologies can be deployed.	Support
Proposal 7–5 The Office of the Privacy Commissioner should provide guidance in relation to technologies that impact on privacy (including, for example, guidance for use of RFID or data collecting software such as 'cookies'). Where appropriate, this guidance should incorporate relevant local and international standards. The guidance should address:	Support, but needs to be linked to requirements for PIAs (see our submission on Pt G Chapter 44). Our sSupport is also subject to reservations about imbalance in many standards setting bodies. Standards should only be considered for adoption where their development has included the direct involvement of organisations representing the interests of consumers and citizens, in particular the

ALRC PROPOSALS	APF SUBMISSION
	privacy interest, with adequate resourcing, and where evidence exists to show that appropriate balance has been achieved
(a) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';	
(b) when the use of a certain technology will require, under the proposed 'Specific Notification' principle, agencies and organisations to notify individuals at or before the time of collection of personal information;	
(c) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometrics systems);	
(d) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information held in an intelligible form (for example, what biometric information is held about an individual when the information is held as an algorithm); and	
(e) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.	
Proposal 7-6 The Office of the Privacy Commissioner should provide guidance to organisations on the privacy implications of data-matching.	Support but GLs (Rules) should be mandatory
Embedded proposal [7.122] - The ALRC proposes that it should **not** be mandatory for agencies to comply with the existing voluntary OPC data-matching guidelines.	Disagree – GLs (Rules) should be mandatory
Invitation for further comment [7.133] – The ALRC is interested in hearing whether the mechanisms proposed is [Chapter 7] provide an adequate and effective framework for addressing the impact of developing technology on privacy. In particular, the ALRC is interested in hearing about any effective regulatory mechanisms that have not been considered in this chapter.	One useful regulatory mechanism for addressing the impact of developing techniology would be a requirement for Privacy Impact Assessment (PIA) – see our submission on PIA in our response to Pt G Chapter 44.

ALRC PROPOSALS	APF SUBMISSION
Ch 8 (Scope of the Privacy Act) Individuals, the Internet, and Generally Available Publications	
Question 8–1 Should the online content regulation scheme set out in the *Broadcasting Services Act 1992* (Cth), and in particular the ability to issue take-down notices, be expanded beyond the *National Classification Code* and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy? If so, what criteria should be used to determine when a take-down notice should be issued? Who is the appropriate body to issue the take-down notice?	No - the take down notice scheme is neither intended, nor suited, for dealing with privacy violations.
Proposal 8–1 The Office of the Privacy Commissioner should provide guidance that relates to generally available publications in an electronic form. This guidance should: (a) apply whether or not the agency or organisation is required by law to make the personal information publicly available; (b) set out certain factors that agencies and organisation should consider before publishing personal information in an electronic form (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and (c) set out requirements in the proposed Unified Privacy principles with which agencies and organisations need to comply when collecting personal information from generally available publications (for example, when a reasonable person would expect to be notified of the fact and circumstances of collection),	Support subject to generic comments on OPC guidance in our Introduction.
Ch 9 – Identity Theft	
No proposals or Questions	See ID theft flag proposal in Part G

DP72 Part B – Developing Technology – Biometric Technology

General Comment

The short section on Biometrics in Chapter 6 does not do full justice to the seriousness and urgency of the subject, which has major privacy implications. Four years ago, the APF's current Chair called for a moratorium on the application of biometric technologies unless and until regulatory mechanisms are in place:
http://www.anu.edu.au/people/Roger.Clarke/DV/Biom030908.html
http://www.anu.edu.au/people/Roger.Clarke/DV/AusCERT0405.html (29-33)
That call has recently been echoed by some within the biometrics industry, for the pragmatic reason that the impacts of poorly implemented schemes will be so severe that biometrics will gain a very poor reputation, as both authoritarian and highly error-prone.
The APF submits that a more detailed discussion paper is required to convey the seriousness and urgency of the issues inherent in biometric authentication and identification, and adequately canvass appropriate responses.

Specific Comments

A crucial factor not reflected in para. 6.690 (p. 332) is whether and where biometrics are stored.

Another consideration that is not reflected is the significantly different uses to which biometrics can be put, in particular authentication of assertions (involving 1-to-1 comparison between a new measure and a previously captured measure) and identification (involving 1-to-many comparisons, and large databases of biometric measures).

It is important that a connection be drawn between this topic and the anonymity and pseudonymity discussion elsewhere (See our submission on proposed UPP1 in our response to Part D of ALRC DP72). Biometrics are an 'entifier', and expressly deny the possibility of having multiple identities each with its own identifier.

The list of privacy concerns in para. 6.70 (p. 332) is incomplete, and the tone fails to convey their seriousness.

The following list is provided in Clarke (2001), at:
http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html#Thr

Privacy of the Person

Biometric technologies don't just involve collection of information about the person, but rather information of the person, intrinsic to them. That alone makes the very idea of these technologies distasteful to people in many cultures, and of many religious persuasions.

In addition, each person has to submit to examination, in some cases in a manner that many people regard as demeaning. For example, the provision of a quality thumbprint involves one's forearm and hand being grasped by a specialist and rolled firmly and without hesitation across a piece of paper or a platen; and an iris-print or a retinal print require the eye to be presented in a manner compliant with the engineering specifications of the supplier's machine. Some technologies, such as those based on DNA, go so far as to require the person to provide a sample of body-fluids or body-tissue.

Privacy of Personal Data

Many schemes require the provision of personal data to assist in the administration of the scheme. Some are operated in close conjunction with other data-rich systems such as personnel or welfare administration. This consolidation of data enhances the opportunity for the organisation to exercise control over the population for whom it holds biometrics.

Privacy of Personal Behaviour

The monitoring of people's movements and actions through the use of biometrics increases the transparency of individuals' behaviour to organisations. Those organisations are in a better position to anticipate actions that they would prefer to prevent and communicating warnings to the predicted perpetrators. Moreover, an organisation that performs biometrics-aided monitoring is in a position to share personal data with other organisations, such as contracted suppliers and customers, 'business partners', and corporations and governments agencies with which it 'enjoys a strategic relationship'.

Multi-Purpose and General-Purpose Identification

Biometric schemes are expensive. They also require the individuals that are subjected to them to register with some authority. Some schemes also require the individual to carry a token such as a card.

To share costs, organisations are therefore motivated to apply biometric schemes for multiple purposes. Any multiple usage of identifiers represents a serious threat to privacy, because it provides the organisations with simple means of sharing the data that each of them gathers, and hence with means to exercise control over the individuals involved.

There are no natural barriers to data-sharing, many countries lack laws to preclude it, and a strong tendency exists for organisations to break down such legal impediments as do exist. Hence the multiple purposes to which a biometric scheme is applied can readily extend beyond a single organisation to encompass multiple organisations in both the private and public sectors.

Denial of Anonymity and Pseudonymity

Until very recent times, the vast majority of actions and transactions undertaken by people were anonymous, or were identified only to the extent that an observer saw them and might remember them, but no records of the event were kept.

Corporations and government agencies have been working very hard to deny people the ability to keep their transactions anonymous. As a result of new forms of information technology, the cost of data capture has plummeted, and huge numbers of transactions are now recorded which would have been uneconomic to record in the past.

These records carry enough information to identify who the person was who conducted them, and systems are designed so as to readily associate the data with that person.

Biometric technologies create new capabilities for the association of identity with transactions that have never been recorded before, such as passing through a door within a building, across an intersection, or into a public place or an entertainment facility. They provide a powerful weapon to corporations and governments, whereby yet more of the remnant anonymity of human action can be stripped away.

Masquerade

The storage of biometrics makes much easier the fabrication of tools, or the synthesis of signals, that are highly convincing replicas of a particular person's physiometrics. This raises the prospect of people having acts attributed to them that they did not do.

The feasibility of the manoeuvre varies depending on the kind of biometric. The technology to fabricate a convincing iris, based on the data captured and stored by an iris-reading device would seem to be challenging, and may well not exist. On the other hand, if a biometric comprises measurements of some part of a person's body, such as the first knuckle of the right thumb, then technology is probably already available that can produce a synthetic equivalent of that body-part.

Moreover, some biometric techniques select a small sub-set of the captured data, such as the number and orientation of ridges on a fingerprint, or the location and size of features in an iris. The risk is all the greater if the biometric is used in its raw form, or the compression is insufficiently `lossy' and hence the compressed form can be used to generate an adequate masquerade, or the hashing algorithm is not one-way.

A significant risk exists that an imposter could produce means to trick devices into identifying or authenticating a person even if they are not present. Possible uses would be to gain access to buildings, software or data, digitally sign messages and transactions, capture the person's identity, harm the person's reputation, or `frame' the person.

Any id or authentication scheme that involves storage of a biometric is fraught with enormous risks. These will very likely rebound on the person, whether or not it harms the organisation that sponsors the scheme.

Permanent Identity-Theft

An act of masquerading as another person is a single event. If the imposter conducts a succession of masquerades, their behaviour amounts to taking over the person's identity. Cases of identity theft have been reported already, which have had very serious consequences for the victims. Organisations cannot

distinguish the acts and transactions of the two individuals using the one identity, and hence they are merged together. A typical outcome is that the person faces demands for payment from organisations they have never purchased anything from, and shortly afterwards can no longer gain access to loans.

Under these circumstances, the identity can become so tainted that the person has to abandon that identity and adopt a new one. That is challenging, because such an act is readily interpreted as an admission of guilt, and an attempt to avoid the consequences of actions that are presumed to be actions of that person, rather than of the imposter.

Biometrics adds a frightening new dimension to identity theft. The purveyors of the technology convey the message that it is foolproof, in order to keep making sales. The organisations that sponsor schemes want to believe that it is foolproof, in order to avoid liabilities for problems. The resulting aura of accuracy and reliability will make it extraordinarily difficult for an individual who has been subjected to identity theft to prosecute their innocence.

Any biometric is an extraordinarily dangerous measure, because it's the equivalent of a PIN that can't be changed. Lose it once, and you're forever subject to masquerade by each person or organisation that gains access to it.

Automated Denial of Identity

Identity theft is not limited to individual criminals. For example, a corporation could apply biometrics to the denial of access to premises by ex-employees, customers previously found guilty of shop-lifting, and in the case of casinos, problem-gamblers.

Proposals of this nature have arisen in the context of football grounds, and it was reported that an application was applied to the thousands of people who streamed into the U.S. Super Bowl in January 2001 (e.g. Green 2001).

The technique could of course be extended to the denial of access by customers suspected of shop-lifting, complainants, or known agitators against the company's practices. Government agencies could find scores of applications, such as preventing targeted people from using transport facilities. This scenario was investigated many years ago in the sci-fi novel 'Shockwave Rider' (Brunner 1975).

Chilling Effect on Freedom, and on Democracy

Biometric technologies, building as they do on a substantial set of other surveillance mechanisms, create an environment in which organisations have enormous power over individuals. Faced with the prospect of being alienated by employers, by providers of consumer goods and services, and by government agencies, individuals are less ready to voice dissent, or even to complain.

That is completely contrary to the patterns that have been associated with the rise of personal freedoms and free, open societies. It represents the kind of closed-minded society that the Soviet bloc created, and which the free world decried. The once-free world is submitting to a 'technological imperative', and permitting surveillance technologies to change society for the worse. Biometrics tools are among the most threatening of all surveillance technologies, and herald the severe curtailment of freedoms, and the repression of 'different-thinkers', public interest advocates and 'troublemakers'.

Clearly, this undermines democracy, because candidates, dependent on parties, sponsors and the media, are less willing to be marginalised; supporters are less prepared to be seen to be so; and voters become fearful of the consequences if their voting patterns become visible.

Less clearly, the suppression of different-thinkers strangles the economy. It does this because the adaptability of supply is dependent on experimentation, choice, and the scope for consumers to change their demand patterns.

Dehumanisation

Beyond the fairly practical considerations of freedom of thought and action, democracy and economic behaviour, there is the question of the ethics of the matter. If we're happy to treat humans in the same manner as manufactured goods, shipping cartons, and pets, then biometrics technologies are unobjectionable. If, on the other hand, humans continue to be accorded special respect, then biometrics technologies are repugnant to contemporary free societies. Authoritarian governments ride rough-shod over personal freedoms and human rights. They will establish legal authority for and enforcement of the capture of biometrics for every transaction, and at every doorway. Such governments see consent and even awareness by the person as being irrelevant, because they consider that the interests of society or 'the State' (i.e. of the currently powerful cliques) dominate the interests of individuals. In the free world as well, substantial momentum exists within governments and corporations to apply those same technologies, and in the process destroy civil rights in those countries.

DP72 Part C – Interaction, Inconsistency and Fragmentation

ALRC PROPOSALS	APF SUBMISSION
PART C – Interaction, Inconsistency and Fragmentation	
Ch 10 – Overview	
No proposals.	
Ch 11 – The Costs of Inconsistency and Fragmentation	
Proposal 11–1 The Office of the Privacy Commissioner should provide further guidance to agencies and organisations on privacy requirements affecting information sharing.	Support subject to our general reservations about OPC guidance in our Introduction.
Proposal 11–2 Agencies that are required or authorised by legislation or a public interest determination to share personal information should develop and publish documentation that addresses the sharing of personal information; and where appropriate, publish other documents (including memoranda of understanding, indemnity agreements and ministerial agreements) relating to the sharing of personal information.	Support – maximum transparency is desirable.
Proposal l 1–3 The Australian Government should convene an inter-agency working group of senior officers to identify opportunities where it would be appropriate to share or streamline the sharing of personal information among Australian Government agencies.	Disagree - It should not be a function of a privacy law to proactively search out data-sharing opportunities – the immediate need is for a standing body to review any such proposals, whatever their origin, in light of privacy obligations – see Proposal 11-4.
Proposal 11–4 The Australian Government, in consultation with state and territory governments, intelligence agencies, law enforcement agencies, and accountability bodies (including the Office of the Privacy Commissioner; the Inspector-General of Intelligence and Security; state and territory privacy commissioners and agencies with responsibility for privacy regulation; and federal, state and territory ombudsman), should: (a) develop and publish a framework relating to cross-border sharing of personal information within Australia by intelligence and law enforcement agencies; and (b) develop memoranda of understanding to ensure that accountability bodies can oversee	Support (see also proposal 64-4 re PC membership of ACMA LEAC)

ALRC PROPOSALS	APF SUBMISSION
cross-border information sharing within Australia by law enforcement and intelligence agencies.	
Question 11–1 Are the definitions of 'contracted service provider' and 'State contract' under the *Privacy Act 1988* (Cth) adequate? For example, do they cover all the types of activities that private sector organisations might perform on behalf of agencies?	
Ch 12 – Federal Information Laws	
Proposal 12–1 The Australian Government and state and territory governments should ensure the consistency of definitions and key terms (for example, 'personal information', 'sensitive information' and 'health information') in federal, state and territory legislation that regulates the handling of personal information.	Support
Proposal 12–2 Section 41(1) of the *Freedom of Information Act 1982* (Cth) should be amended to provide that a document is exempt if: (a) it contains personal information, the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle and disclosure would not, on balance, be in the public interest; or (b) it contains personal information of a deceased individual, the disclosure of that information would constitute a breach of the proposed 'Use and Disclosure' principle (but where the Principle would require consent the agency must consider whether the proposed disclosure would involve the unreasonable disclosure of personal information about any individual including the deceased individual) and disclosure would not, on balance, be in the public interest.	Support in principle subject to new developments in overall information law
Proposal 12–3 'Personal information' should be defined in the *Freedom of Information Act 1982*(Cth) as 'information or an opinion, whether true or not and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.	Support (but see our previous submission on ALRC IP31 re 'personal affairs' information).
Proposal 12–4 The *Freedom of Information Act 1982* (Cth) should be amended to require that the body that is primarily responsible for administration of the Act is to: (a) develop and publish guidelines on the interpretation and application of s41;	Support – we note that the new Government proposes to integrate the functions of the Privacy Commissioner with those of a new Information Commissioner – see our comments on this new environment in our Introduction

ALRC PROPOSALS	APF SUBMISSION
(b) consult with the OPC before issuing guidelines on the interpretation and application of s 41.	
Proposal 12–5 The *Freedom of Information Act 1982*(Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act 1982* (Cth) is a disclosure that is required or authorised for the purposes of the proposed 'Use and Disclosure' principle under the Privacy Act	Support
Proposal 12–6 The *Privacy Act 1988* (Cth) should be amended to provide a new Part dealing with access to, and correction of, personal information held by an agency.	Support in principle subject to new developments in overall information law
Proposal 12–7 The *Freedom of Information Act 1982*(Cth) should be amended to: (a) provide that an individual's right to access or correct his or her own personal information is dealt with under the Privacy Act; (b) delete part V of the Act.	Support in principle subject to new developments in overall information law
Proposal 12–8 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that: (a) if an agency holds personal information about an individual , the agency must, if requested by the individual, provide the individual with access to the information, subject to a number of exceptions under the Part; (b) where an individual is given access to personal information, the individual must be advised that he or she may request the correction of that information; (c) where an agency is not required to provide the individual with access to personal information because of an exception, the agency must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary , provided that the compromise would allow for sufficient access to meet the needs of both parties; and (d) nothing in the Part is intended to prevent or discourage agencies from publishing or giving access to personal information, otherwise than as required by the Part, where	Support (should generally replicate UPP 9 – any differences to be justified)

ALRC PROPOSALS	APF SUBMISSION
they can do so properly or are required to do so by law.	
Question 12–1 What exceptions should apply to the general provision granting an individual the right to access his or her own personal information? For example, should the exceptions mirror the provisions in Part IV of the *Freedom of Information Act 1982* (Cth) or should another set of exceptions apply?	Should generally replicate UPP 9 – any differences to be justified
Proposal 12–9 The proposed Part of the *Privacy Act* dealing with access to, and correction of, personal information held by an agency should provide that if an agency holds personal information about an individual the agency must: (a) if requested by the individual take such steps to correct (by way of making appropriate corrections, deletions and additions) the information as are in the circumstances, reasonable to ensure that the information is, with reference to a purpose of collection permitted by the UPPs, accurate, complete, up-to-date, relevant and not misleading; (b) where the agency has taken the steps outlined in (i) above, if requested to do so by the individual, and provided such notification would be practicable in the circumstances, notify any other entities to whom the personal information has already been disclosed before correction.	Should generally replicate UPP 9 – any differences to be justified
Proposal 12-10 The proposed part of the *Privacy Act* dealing with access to, and correction of personal information held by an agency should provide that where an agency decides not to correct the personal information of an individual and the individual requests the agency to annotate the personal information with a statement by the individual claiming that the information is not accurate, complete , up-to-date, relevant, or is misleading the agency must take reasonable steps to do so.	Should generally replicate UPP 9 – any differences to be justified
Proposal 12–11 The proposed Part of the Privacy Act dealing with access to, and correction, of personal information held by and agency should set out a process for dealing with a request to access or correct personal information that addresses: (a) the requirements for making an application for correction or annotation of personal information;	Should generally replicate UPP 9 – any differences to be justified

ALRC PROPOSALS	APF SUBMISSION
(b) time periods for processing a request to access or correct personal information; (c) the transfer of a request to access or correct personal information to another agency in certain circumstances (for example, when a document is not in the possession of an agency but is, to the knowledge of that agency in the possession of another agency); (d) how personal information is to be made available to the individual (including by giving a reasonable opportunity to inspect the records, by providing a copy of the record, by giving a summary of the contents of the record, by providing oral information about the contents of the record); (e) how corrections are to be made (including by additions and deletions); (f) the deletion of excepted matter or irrelevant material; (g) the persons authorised to make a decision on behalf of an agency in relation to a request to access or correct personal information; (h) when a request for access to personal information may be refused by an agency(for example, when it would substantially and unreasonably divert the resources of the agency from its other operations, or in the case of a Minister, would substantially and unreasonably interfere with the performance of the Minister's functions); and (i) the provision of reasons for a decision to deny a request to access or correct personal information.	
Proposal 12-12 The Proposed Part of the Privacy Act dealing with access to, and correction of, personal information held by an agency should provide for: (a) internal review by an agency of a decision made under the Part; (b) review by the Administrative Appeals Tribunal of a decision made under the Part (including the power to make an order for compensation); and (c) complaints to the Commonwealth Ombudsman.	Support
Proposal 12-13 The Office of the Privacy Commissioner should issue guidelines on access to,	Support subject to general reservations about OPC guidance in our

ALRC PROPOSALS	APF SUBMISSION
and correction of records containing personal information held by an agency.	Introduction.
Question 12-2 Should the Office of the Privacy Commissioner's complaint handling, investigative and reporting functions be exempt under the *Freedom of Information Act 1982* (Cth)	No – only whatever generic exemptions for complaint bodies will apply
Proposal 12-14 Part VIII of the Privacy Act 1988 (Cth) (obligations of confidence) should be repealed.	Support
Chapter 13 Required or Authorised under Law	
Question 13-1 Should the definition of 'law' for the purposes of determining when an act or practice is required or specifically authorised by or under a law include: (a) common law or equitable duty; (b) an order of a court or tribunal; (c) documents that are given the force of law by an Act of Parliament, such as industrial awards; (d) statutory instruments such as a Local Environmental Plan made under a planning law?	Yes to all in principle. Needs to cross refer to proposal for 'specifically' authorised in the UPPs – see our submission on Part D.
Question 13-2 Should a list be compiled of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*? If so, should the list have the force of law? Should it be comprehensive or indicative? What body should be responsible for compiling and updating the list?	Exhaustive list impracticable, but a list of most common requirements would be useful – OPC to compile
Proposal 13-1 If the exemption that applies to registered political parties and political acts and practices is not removed, the Commonwealth Electoral Act 1918(Cth) should be amended to provide that prescribed individuals, authorities and organisations to whom the Australian Electoral Commission must give information in relations to the electoral roll and certified lists of voters must take reasonable steps to: (a) protect the information from misuse and loss and from unauthorised access, modification or disclosure; and	Support (but exemption should go – see our submission on Part E)

ALRC PROPOSALS	APF SUBMISSION
(b) destroy or render the information non-identifiable if it is no longer needed for a permitted purpose.	
Proposal 13-2 The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, should develop and publish protocols that address the collection, use and destruction of personal information shared for the purposes of the continuous update of the electoral roll.	Strongly support
Proposal 13-3 The review of the *Anti-Money Laundering and Counterterrorism Financing Act 2006* (Cth), the regulations and the Anti-Money Laundering and Counter-terrorism Financing Rules under s 251 of the Act should consider, on particular, whether: (a) reporting entities and designated agencies are appropriately handling personal information under the legislation; (b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation; © it remains appropriate that reporting entities are required to retain information for seven years; and (d) it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification.	Strongly support
Proposal 13-4 The Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Cth) should be amended to provide that state and territory agencies that access personal information provided to the Australian Transaction Reports and Analysis Centre under the Act be regulated under the *Privacy Act* in relation to the handling of that personal information, except where they are covered by obligations under a state of territory law that are, overall, at least the equivalent of all the relevant obligations in the *Privacy Act*.	Strongly support
Ch 14 – Interaction with State and Territory Laws	
Proposal 14–1 The *Privacy Act* should be amended to provide that when an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies (for example a Ministerial Council), the Australian	Support

ALRC PROPOSALS	APF SUBMISSION
Government agency should ensure that a memorandum of understanding is in place so that the intergovernmental body and its members do not act, or engage in a practice, that would breach the Act.	

DP72 Part D – The Privacy Principles

ALRC PROPOSALS	APF SUBMISSION
PART D – Unified Privacy Principles	
Ch 15 – Structural Reform of Privacy Principles	
Proposal 15–1 The privacy principles in the Privacy Act should be drafted to pursue, as much as practicable, the following objectives: (a) the obligations in the privacy principles generally should be expressed as high level principles; (b) the privacy principles should be simple, clear and easy to understand and apply; and (c) the privacy principles should impose reasonable obligations on agencies and organisations.	We support Proposal 15-1. However we believe that it is also desirable to adopt principles (i) which are consistent, at least within Australia, and (ii) which represent best practice in internationally accepted privacy standards
Proposal 15–2 The Privacy Act should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles—the Unified Privacy Principles (UPPs)—that would be generally applicable to agencies and organisations, subject to such exceptions as required.	We support Proposal 15-2.
Proposal 15–3 The proposed UPPs should apply to information privacy except to the extent that: (a) the Privacy Act or another piece of Commonwealth primary legislation imposes different or more specific requirements in a particular context; or (b) subordinate legislation under the Privacy Act imposes different or more specific requirements in a particular context.	We support Proposal 15-3.
Proposal 15–4 The National Privacy Principles should provide the general template in drafting and structuring the proposed UPPs.	

ALRC PROPOSALS	APF SUBMISSION
Ch 16 – Consent	
Proposal 16–1 The Office of the Privacy Commissioner should provide further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should: (a) cover consent as it applies in various contexts; and (b) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.	The definition of 'consent' should be amended to deal with a number of key issues concerning consent, specified in the following submissions, rather than leaving them to OPC guidance. Other aspects of consent should be dealt with where possible in the Explanatory Memorandum, and only otherwise by OPC guidance. Any OPC guidance should be required to be issued within one year. In relation to implied consent, either the definition of 'consent' or the explanatory memorandum should state that implied consent must be clear and not ambiguous. Either the Act or the Explanatory Memorandum should state that a failure to opt out is not by itself to constitute consent. The Act or the Explanatory Memorandum should state that where a person has no choice but to provide personal information in order to obtain a benefit, no consent to any uses of the information beyond the express purpose of collection may be implied. In such circumstances of 'involuntary consent', only express consent should apply. The definition of 'consent' needs to be amended in order to prevent abuse of the practice of 'bundled consent'. In particular, wherever consent is applicable to the operation of a privacy principle, separate consent should be required for each proposed purpose of use.
Embedded Question – Should the definition of consent be amended? (ALRC 16.2)	Yes – see our response to Proposal 16-1
Embedded Question – Should the proposed UPPs contain a separate principle that deals with the issue of consent? (ALRC 16.2)	No - see our response to Proposal 16-1

ALRC PROPOSALS	APF SUBMISSION
Ch 17 – Anonymity and Pseudonymity	
Proposal 17-1 The proposed Unified Privacy Principles should contain a principle called 'Anonymity and Pseudonymity' that sets out the requirements on agencies and organisations in respect of anonymous and pseudonymous transactions with individuals.	Support UPP 1 should state that 'agencies and organisations must give individuals the option of anonymity/pseudonymity, not that 'individuals … should have' this option. (This reformulation is also necessary in relation to our submission on proposal 17-2).
Proposal 17-2 The proposed 'Anonymity and Pseudonymity' principle should include a pseudonymity requirement that when an individual is transacting with an agency or organisation, the agency or organisation must give the individual the option of identifying himself or herself by a pseudonym. This requirement is limited to circumstances where providing this option is lawful, practicable and not misleading.	Support – see 17-1
Proposal 17-3 The proposed 'Anonymity and Pseudonymity' principle should provide that, subject to the relevant qualifications in the principle, an agency or organisation is required to give individuals the clear option to transact anonymously or pseudonymously.	Support 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 or agency – they must be able to be tested by an independent party. The anonymity principle should impose an obligation on organisations to facilitate, where practicable and lawful, anonymous or pseudonymous transactions between individuals and third parties The words '..,provided this is not misleading' should be deleted from paragraph (b) of UPP1. APF endorses the revised wording for UPP1 proposed by the Cyberspace Law & Policy Centre.

ALRC PROPOSALS	APF SUBMISSION
Proposal 17-4 The Office of the Privacy Commissioner should provide guidance to agencies and organisations on: (a) when it is and is not lawful and practicable to give individuals the option to transact anonymously or pseudonymously; (b) when it would be misleading for an individual to transact pseudonymously with an agency or organisation; and (c) what is involved in providing a clear option to transact anonymously or pseudonymously.	Support
Ch 18 – Collection	
Proposal 18–1 (a) The proposed Unified Privacy Principles should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned. (b) The Office of the Privacy Commissioner should provide guidance to clarify when it would not be reasonable and practicable to collect such information from the individual concerned.	Support both subject to our general comments about OPC guidance in our Introduction . The ALRC should address the issue of how Australian law should clarify the relationships between collection and disclosure of personal information, and in particular the limitations that the purposes of collection of a first organisation play in limiting the uses of a second organisation to which the information is disclosed. If this is not done in the legislation, it would nevertheless be valuable to have the Explanatory Memorandum clarify what is the expected interpretation of the legislation. The ALRC should also address the issue of the role that the law of breach of confidence plays in determining the circumstances under which the use or disclosure of personal is limited.
Proposal 18–2 The 'Collection' principle in the proposed Unified Privacy Principles (UPPs) should provide that, where an agency or organisation receives unsolicited personal information, it must either; (a) destroy the information immediately without using or disclosing it; or (b) comply with all relevant provisions in the UPPs that apply to the information in questions, as if the agency or organisation had taken active steps to collect the information.	We support this qualified application of the collection principle to unsolicited information, provided it is made clear that 'using or disclosing' includes taking *any* action, and that the destruction option must be exercised within a very limited time – otherwise it would be essential for at least the security principle to apply while the information was held. The Act or Explanatory Memorandum should make it clear that unsolicited information is included within the meaning of 'collect'. We comment further below on other means of collection. The law should make it clear that the collection principles UPPs 1

ALRC PROPOSALS	APF SUBMISSION
	and 2 apply to the maximum practical extent to information obtained from observation or surveillance; to information extracted from other records, and to information generated within an organisation or agency as a result of transactions. This should be done either in the legislation or in the Explanatory Memorandum.
Proposal 18–3 The 'Collection' principle in the proposed Unified Privacy Principles should provide that an agency or organisation must not collect personal information unless it reasonably believes the information is necessary for one or more of its functions or activities.	While we support the inclusion of this additional test, we believe that overall the obligation remains too subjective, and that further guidance is desirable within the principle itself concerning several of the other criteria. We make the following suggestions: • Add to UPP 2.1 the words '…and is proportional to those functions or activities'. • Add to UPP 2.1 a second sentence: 'The perceived necessity must be related to the particular purpose of collection of the information in question.'. • UPP 2.1 should refer to 'one or more of its lawful functions or activities.'. .
Ch 19 – Sensitive Information	
Proposal 19–1: The proposed Unified Privacy Principles should set out the requirements on agencies and organisations in relation to the collection of personal information that is defined as 'sensitive information' for the purposes of the *Privacy Act*…	
…These requirements should be located in the proposed 'Collection' principle.	The ALRC proposes to include the substantive content of NPP10 into the new collection UPP (2.6), where it will apply to both organisations and agencies (ALRC DP 72 Chapters 18 & 19). We support this in principle, but have some reservations concerning the exceptions. The consent exception in UPP 2.6(a) should require express or explicit consent. The first paragraph of UPP 2.6(d) should read 'if the information is

ALRC PROPOSALS	APF SUBMISSION
	collected in the course of the lawful activities of a non-profit organisation that has aims relating to sensitive information (as defined in this Act) – the following conditions are satisfied:' The Privacy Commissioner should be required to issue guidance about fair and lawful means of collection, which are of considerable practical importance.
Proposal 19–2: The proposed sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or specifically authorised by or under law.	The exception (b) in UPP 2.6 should include the word 'specifically'.
Proposal 19–3: The proposed sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is incapable of giving consent.	Disagree - We oppose the deletion of the word 'imminent' from UPP 2.6(c)
Question 19-1 Should the proposed sensitive information provisions provide that sensitive information can be collected where all of the following conditions apply: (a) the individual is incapable of giving consent; (b) the collection is necessary to provide an essential service for the benefit of the individual; and (c) the collection would be reasonable in all the circumstances?	No - this is unnecessary.
Ch 20 – Specific Notification	
Proposal 20–1 The proposed Unified Privacy Principles should contain a principle called 'Specific Notification' that sets out the requirements on agencies and organisation to provide specific notification to an individual of particular matters relating to the collection and handling of personal information about the individual.	Support
Proposal 20-2 The proposed 'Specific Notification' principles should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual, it must take reasonable	We support the ALRC's suggestion (explained in paragraph 20.30) that the notification requirements should generally apply to all circumstances of collection. In our view this should *expressly*

ALRC PROPOSALS	APF SUBMISSION
steps to ensure that the individual is aware of the: (a) fact and circumstances of collection (for example, how, when and from where the information was collected); (b) identity and contact details of the agency or organisation; (c) fact that the individual is able to gain access to the information; (d) purposes for which the information is collected; (e) main consequences of not providing the information; (f) types of people, organisations, agencies or other entities to whom the agency or organisation usually discloses personal information; and (g) avenues of complaint available to the individual if he or she ahs a complaint about the collection or handling of his or her personal information. This requirement should only apply : (1) in circumstances where a reasonable person would expect to be notified; (2) except to the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual; and (3) subject to any other relevant exceptions.	include collection by observation, surveillance or internal generation in the course of transactions (see our comments below on UPP 3.1(a) and also on these different modes of collection in relation to UPP 2), UPP 3 should read: '…..from the individual, by whatever means, it must take …' We are concerned that leaving the obligation as 'ensuring awareness' (as in NPP 1.3) is too open to abuse. For instance, as we have argued previously (in relation to our IP 31 submission, 4-2), data users could deliberately omit privacy notices from routine communications even where there is minimal marginal cost in repeating it, relying instead on an initial communication constituting 'reasonable steps'. In our view, it is asking too much of individuals to expect them to remember the details of a privacy notice several months after they have received it, and in most contexts there is no good reason why notice should not be repeated. We agree that the objective of this principle is to ensure awareness, but a better way of consistently achieving this objective would be, in our view, to change this principle from one of reasonable steps to 'ensure awareness' to reasonable steps to specifically 'notify', with a conditional exception where the data user could establish that at least the typical data subject had been made aware by other means (see our comment on UPP 3.1(a) below. UPP 3.1 should be re-worded from '… reasonable steps to ensure that the individual is aware' to '…reasonable steps to notify the individual…' UPP 3.1(c) should read 'fact that the individual is able to gain access to the information and seek correction;' Proposed UPP 3.2(b) should be amended to read: 'the identity of the source of the information, if requested by the individual.'

ALRC PROPOSALS	APF SUBMISSION
Proposal 20-3 The Office of the Privacy Commissioner should provide guidance to assist agencies and organisation in ensuring that individuals are properly informed of the persons to whom their personal information is likely to be disclosed.	Supported, however, far more of the detail of what the requirements mean in practice should be incorporated in the principle itself, leaving less to be covered in the guidance. The Privacy Commissioner should be required to issue guidance about compliance with the specific notification requirements under UPP 3 in relation to different circumstances of collection. Proposed UPP 3.2 should be amended at the end of the first paragraph to read '… the individual is or has been made aware, at or before the time of that collection (or, if that is not practicable, as soon as practicable thereafter) of:'
Proposal 20–4 An agency should be required to notify an individual of the matters listed in the proposed 'Specific Notification' principle, except to the extent that the agency is required or specifically authorised by or under law not to make the individual aware of such matters.	We support the proposed exception UPP 3.3(b)(ii) but submit that it should apply both to agencies and to organisations.
Proposal 20–5 (a) The proposed 'Specific Notification' principle should provide that where an agency or organisation collects personal information from someone other than the individual concerned, it must take reasonable steps to ensure that the individual is or has been made aware of: (1) the matters listed in Proposal 20-2; and (2) on request by the individual, the source of the information. (b) this requirement should only apply: (1) in circumstances where a reasonable person would expect to be notified; (2) except the extent that making the individual aware of the matters would pose a serious threat to the life or health of any individual; and (3) in the case of an agency, except to the extent that it is required or specifically authorised by or under law not to make the individual aware	We are concerned at the suggestion in paragraph 20.33 that there will be a broad range of circumstances where no notification will be necessary. We believe that the case made here is far too simplistic. Just because an individual is aware that collection is taking place does not automatically mean that they are aware of all of the matters to be included in normal notifications, and even if they have previously been notified, some of the details (such as intended recipients) may have changed over time. Any exceptions should be narrow and specific. The exception embodied in UPP 3.3(a) is, in our view, far too subjective and also adopts the wrong 'default' setting. To the extent that an exception based on 'prior expectation' is justified, this should clearly *be* the exception; i.e. notification should be required *unless* there is a reasonable belief that most of the individuals concerned would not expect to be notified. Such a belief would most commonly be founded on a claim that individuals had already been made aware in some other way. There may also be some circumstances in which such a belief could be founded on evidence that individuals were not

ALRC PROPOSALS	APF SUBMISSION
of one or more of these matters.	interested in knowing, although this could be more difficult to establish. UPP 3.3 should be re-worded as follows: 'An agency or organisation must comply with the obligations in UPPs 3.1 and 3.1 unless: (a) it reasonably believes that there is a reasonable expectation on the part of individuals concerned that they not be notified The ALRC proposes an exception where making the individual aware would pose a serious threat to the life or health of any individual. (ALRC DP 72, [20.25], and UPP 3.3(b)(i). This carries over an existing exception to NPP 1.5, but would apply not only to collection from third parties but also to collection directly from the individual. There is no such current exception to NPP 1.3, and the ALRC has not provided any arguments to support this extension. Given that in the direct collection situation the individual will be aware that information is being collected, it seems unlikely that informing them of the matters covered by UPP 3.1 could cause any additional harm. In the absence of any justification, we oppose the application of exception (b)(i) to direct collection. UPP 3.3(b)(i) should only apply to indirect collection. As such, it may be better relocated to UPP 3.2. The ALRC also proposes that UPP 3 should contain a further exception – that an agency not be required to comply with the relevant notification requirements if it is 'required or specifically authorised by or under law' not to make the individual aware, (ALRC DP 72, [20.23] and proposed UPP3.3(b)(ii)). Under the ALRC proposal, this exception would not be available to private sector organisations. We cannot see why it should not – there are such statutory constraints on businesses, such as the

ALRC PROPOSALS	APF SUBMISSION
	prohibition on 'tipping off' in the AML-CTF Act 2006 (s123). We therefore support the proposed exception UPP 3.3(b)(ii) but submit that it should apply to agencies and organisations.
Proposal 20–6 The Office of the Privacy Commissioner should provide guidance on the circumstances in which it is necessary for an agency or organisation to notify an individual when it has received personal information abut the individual from a source other than the individual concerned.	We support the ALRC proposal that the OPC should provide guidance on this aspect of compliance with UPP 3 However, as we have suggested above, far more of the detail of what the requirements mean in practice should be incorporated in the principle itself, leaving less to be covered in the guidance.
Proposal 20–7 The Office of the Privacy Commissioner should provide guidance on the meaning of the 'reasonable steps' in the context of an agency's or organisation's obligation to fulfil its notification requirements under the proposed 'Specific Notification' principle.	We support the ALRC proposal that the OPC should provide guidance on this aspect of compliance with UPP 3. However, as we have suggested above, far more of the detail of what the requirements mean in practice should be incorporated in the principle itself, leaving less to be covered in the guidance.
Ch 21 – Openness	
Proposal 21-1 The proposed Unified Privacy Principles should contain a principle called 'Openness' that sets out the requirements on an agency or organisation to operate openly and transparently by providing general notification in a Privacy Policy of how it manages personal information and how personal information is collected, held, used and disclosed by it.	Support. However, 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) (ALRC DP 72 [21.19]). We disagree. We accept that there has been relatively little use of the Commonwealth (and ACT) Personal Information Digests over the 17 years they have been published. However, they remain a potentially valuable resource for the media and public interest groups to make comparisons and hold governments to account. Agencies will have to prepare the equivalent of a Digest entry in any case to satisfy UPP4, so the marginal cost is only that of annual submission and the compilation by the Privacy Commissioner. Now that these processes are established, the savings from removing the obligation would be very small, while a potentially extremely

ALRC PROPOSALS	APF SUBMISSION
	valuable resource would be lost. UPP 4 should include a requirement: 'an agency must submit an electronic copy of its privacy policy to the Privacy Commissioner at least once each year'. Any privacy policies submitted to the Privacy Commissioner should be published by the Privacy Commissioner, and may be republished by other parties'. We also support a requirement for both agencies and organisations to provide further details of their information management to the Privacy Commissioner on request. This obligation is best located elsewhere in the Act and we take it up in our submission on Part F of DP 72.
Proposal 21-2 The Privacy Policy in the proposed 'Openness' principle should set out an agency's or organisation's policies on the management of personal information, including how the personal information is collected, held, used and disclosed. This document should also include: (a) what sort of personal information the agency or organisation holds; (b) the purposes for which personal information is held; (c) the avenues of complaint available to individuals in the event that they have a privacy complaint; (d) the steps individuals may take to gain access to personal information about them held by the agency or organisation; (e) the types of individuals about whom records are kept; (f) the period for which each type of record is kept; and (g) the persons, other than the individual, who can access personal information and the conditions under which they can access it.	Support.

ALRC PROPOSALS	APF SUBMISSION
Proposal 21-3 The Office of the Privacy Commissioner should issue guidance on how agencies and organisations can comply with their obligations in the proposed 'Openness' principle to produce and make available a Privacy Policy.	Support.
Proposal 21-4 An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the proposed 'Openness' principle, available without charge to an individual: (a) electronically (for example, on its website, if it possesses one); and (b) in hard copy, on request.	Support.
Proposal 21-5 The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the Privacy Act.	APF, like many other consumer representative organisations, while acknowledging an 'information overload' problem, views trends towards layered and short form privacy notices with suspicion, as they can too easily omit information which should be relevant to an individual's decision whether to proceed with a transaction. We believe that it is necessary to mandate a minimum level of information to be provided at or before the time of collection and a minimum standard of transparency and ease of navigation between specific collection notices and privacy policies. This is best achieved either in Regulations or a binding Code. Regulations or a binding Code should prescribe the minimum set of information which needs to be provided at or before the time of collection to achieve the objective of the specific notification principle (UPP 3) and the minimum standard of transparency of links to more detailed information provided under UPP 4.
Ch 22 – Use and Disclosure	
Proposal 22–1 The proposed Unified Privacy Principles should contain a principle called 'Use and Disclosure' that sets out the requirements on agencies and organisations in respect of the use or disclosure of personal information for a purpose other than the primary purpose of collecting the information.	Support 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.

ALRC PROPOSALS	APF SUBMISSION
	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 The law should be clarified to expressly allow for the declaration of multiple specific purposes, but not to allow a broadly stated purpose.
Proposal 22–2 The proposed 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the: (a) secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the primary purpose of collection; and (b) individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.	Support.
Proposal 22–3 The proposed 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose (the secondary purpose) other than the primary purpose of collection if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety.	The arguments put forward to support the removal of the word 'imminent' in this exception have in our view been largely addressed by the 'emergencies and disasters' amendments to the Privacy Act in late 2006 [2]. Only if it becomes evident over time that these amendments have not adequately addressed the concerns should further amendments, such as a major broadening of this exception, be considered. We oppose the deletion of the qualifying word 'imminent' from UPP 5.1(c)
Question 22–1 Should the proposed 'Use and Disclosure' principle contain an exception allowing an agency or organisation to use or disclose personal information for a purpose other than the primary purpose of collection where this is 'required or *specifically* authorised by or under law' instead of simply 'required or authorised by or under law'?	We agree with the reasoning of the ALRC that lead to this proposal, and support the narrower wording. No compelling examples have been provided in support of the status quo.

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

ALRC PROPOSALS	APF SUBMISSION
	We support a narrowing of the proposed exception UPP 5.1 (e) to include 'specifically'.
UPP 5. Use and Disclosure 5.1 An agency or organisation must not use or disclose personal information about an individual for a purpose (the ***secondary purpose***) other than the primary purpose of collection unless: (a) both of the following apply: (i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection; and (ii) the individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose; or (b) the individual has consented to the use or disclosure; or (c) the agency or organisation reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to: (i) an individual's life, health or safety; or (ii) public health or public safety; or (d) the agency or organisation has reason to suspect that unlawful activity has been, is being or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities; or (e) the use or disclosure is required or authorised by or under law; or (f) the agency or organisation reasonably believes that the use or disclosure is necessary for one or more of the following by or on behalf of an enforcement body: (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a	We support the proposed exception UPP 5.1 (f). We suggest that there should be a Note to this exception stating that it requires the active involvement of an Australian enforcement body There should be a clear statement, either by note in the Act (the preferred option) or in the Explanatory Memorandum in relation to UPP 5 that all the exceptions apart from (e) are discretionary and are neither a requirement nor an authorisation to use or disclose.

ALRC PROPOSALS	APF SUBMISSION
prescribed law; (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; (iii) the protection of the public revenue; (iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; (v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal. 5.2 UPP 5.1 operates in respect of personal information that an organisation that is a body corporate has collected from a related body corporate as if the organisation's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information. **Note:** Agencies and organisations are also subject to the requirements of the 'Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.	
Embedded position: Missing Persons - "The ALRC does not believe it is desirable to create further specific exceptions in respect of missing persons... where an agency or organisation has a legitimate reason to search for *a missing person*, it may often be able to avail itself of one of the other exceptions in the use and disclosure principle, or it may seek a public interest determination" (para 22.80)	Support.
Embedded position: Due Diligence - "There is no need to create a new exception dealing with the use and disclosure of personal information in the course of due diligence… guidance already provided by the OPC, especially in Information Sheet 16, is sufficient." (para 22.100)	Support.
Embedded Position: Logging Disclosures - "The ALRC does not believe that it is desirable to require agencies and organisations to record their use of disclosure of personal information when this occurs for a purpose other than the primary purpose of collection" (para 22.115)	UPP 5 should include a specific requirement to keep a log or record of all uses and disclosures for secondary purposes under exceptions (a)-(f
Ch 23 – Direct Marketing	
Proposal 23–1 The proposed Unified Privacy Principles should regulate direct marketing by organisations in a discrete privacy principle, separate from the 'Use and Disclosure' privacy	Support.

ALRC PROPOSALS	APF SUBMISSION
principle. This principle should be called 'Direct Marketing' and it should apply irrespective of whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing.	The Privacy Act should define 'direct marketing' as 'the marketing or promotion of goods, services or ideas, including fundraising and recruitment, by direct targeted communication with specific individuals or by individualised communications, by any means.'
Question 23–1 Should agencies be subject to the proposed 'Direct Marketing' principle? If so, should any exceptions or exemptions apply specifically to agencies?	We believe it should so apply on the grounds that the boundaries between private and public sectors are increasingly blurred, and government agencies are now commonly undertaking direct marketing activities. 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.
Proposal 23–2 The proposed 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.	This should go without saying – it must always remain possible for specific legislation to override generic laws. However, we suggest that the ALRC should not remain neutral, but should instead recommend that any sectoral legislation addressing direct marketing should as far as possible be consistent with UPP 6, and that any weakening of the standards in UPP 6 should be clearly justified.
Proposal 23–3 The proposed 'Direct Marketing' principle should require organisations to present individuals with a simple means to opt out of receiving direct marketing communications.	We support this proposal, but suggest that it is strengthened in a number of ways. (We also suggest that the ALRC reviews the construction of 6.1 with a view to avoiding the double negatives in conditions (b) & (c), which make it quite difficult to understand). UPP 6.1(e) should be amended to read '….each communication by the [organisation] with the individual includes a functional means of contacting the [organisation]. If the communication is by electronic means, the means of contact must be at least as easy to use. UPP 6.1(c) should be amended to read 'the individual has not made

ALRC PROPOSALS	APF SUBMISSION
	a request, either directly or indirectly, to the [agency or] organisation …
Proposal 23–4 The proposed 'Direct Marketing' principle should provide that an organisation involved in direct marketing must comply, within a reasonable time, with an individual's request not to receive direct marketing communications.	Support, but urge that it be strengthened by the prescription, in Regulations or a binding Code, of specific target response times for different media of communication. Either Regulations or a binding Code should prescribe specific response times for different media of communication, to give effect to individuals' requests not to receive further direct marketing communications.
Proposal 23–5 The proposed 'Direct Marketing' principle should provide that an organisation involved in direct marketing must, when requested by an individual to whom it has sent direct marketing communications, take reasonable steps to advise the individual from where 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 [23.62]. UPP 6.3 should be amended to read '…to advise the individual of the identity of the source of the individual's personal information.'
Proposal 23–6 The Office of the Privacy Commissioner should issue guidance to organisations involved in direct marketing, which should: (a) highlight their obligation to maintain the quality of any database they hold containing personal information and assists them in achieving this requirement; and (b) clarify their obligations under the Privacy Act in dealing with particularly vulnerable people, such as elderly individuals and individuals aged 14 and under.	We support this proposal, but suggest that there will also be a need for advice on how to implement the requirements of UPP 6 in relation to specific communications media – in particular the difficulties of communicating much detail when using voice telephony and SMS/MMS or instant messaging. The Privacy Commissioner should be required to issue guidance about compliance with UPP 6, including specifically the matters specified in proposal 23-6, and the practicalities of compliance when using different communications media.
Ch 24 – Data Quality	
Proposal 24-1 The proposed Unified Privacy Principles (UPPs) should contain a principle	Support

ALRC PROPOSALS	APF SUBMISSION
called 'Data Quality' that applies to agencies and organisations.	
Proposal 24-2 The proposed 'Data Quality' principle should require an agency or organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is, with reference to a purpose of collection permitted by the proposed UPPs, accurate, complete, up-to-date and relevant.	There should be a clear statement, either by note in the Act (the preferred option) or in the Explanatory Memorandum that in assessing what steps are reasonable under UPP 7, primary regard shall be given to the extent to which data-processing error can have detrimental consequences in the context of the particular information and circumstances. UPP 8.2 should state "An agency or organisation must take reasonable steps to make sure that the personal information it uses or discloses for a purpose other than the purpose of collection is accurate, complete, up-to-date and relevant in relation to that purpose, unless it is required by law to disclose the information."
Ch 25 – Data Security	
Proposal 25–1 The proposed Unified Privacy Principles should contain a principle called 'Data Security' that applies to agencies and organisations.	
Proposal 25–2 The proposed 'Data Security' principle should require an agency or organisation to take reasonable steps to ensure that personal information it discloses to a person pursuant to a contract, or otherwise in connection with the provision of a service to the agency or organisation, is protected from being used or disclosed by that person otherwise than in accordance with the Unified Privacy Principles.	Support UPP8 should be re-worded to require protection against 'improper access, use, alteration, deletion or disclosure, or other misuse, by both authorised users and by other parties'. (adds other misuse) UPP 8 should also state that 'For the purposes of this Principle, reasonable steps must be proportional to the likelihood and severity of the harm threatened and the sensitivity of the information.'
Proposal 25–3 The Office of the Privacy Commissioner should provide guidance about the meaning of the term 'reasonable steps in the context of the proposed 'Data Security' principle. Matters that could be dealt with in this guidance include: (a) the inclusion of contractual provisions binding a contracted service provider of an agency or organisation to handle personal information consistently with the Unified Privacy	OPC should be required by the Act to issue guidelines on the meaning of 'reasonable steps' within one year.

ALRC PROPOSALS	APF SUBMISSION
Principles; (b) technological developments in this area and particularly in relation to relevant encryption standards; and (c) the importance of training staff adequately as to the steps they should take to protect personal information.	
Proposal 25-4 The proposed 'Data Security' principle should require an agency or organisation to take reasonable steps to destroy or render non-identifiable information if it is no longer needed for any purpose permitted by the Unified Privacy principles, except to the extent that the agency or organisation is required or specifically authorised by or under law to retain the personal information.	We support ALRC proposal 25-4, for a principle 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. UPP 8(b) should be a separate Data Retention principle The data retention principle (whether part of UPP 8 or separate) should provide that personal information must only be retained for any secondary purpose for which it has already legitimately been used, or for which there is express legal authority for retention. A Note should explain that secondary purposes for which personal information may be used or disclosed in future do not provide an alternative justification for retention The obligation in UPP 8(c) should apply to all 'personal information it discloses to a third person'. The obligation in UPP 8(c) should extend to requiring third party recipients of personal information to observe all relevant UPPs in relation to that information.
Proposal 25–5 The Office of the Privacy Commissioner should provide guidance about when it is appropriate for an agency or organisation to destroy or render non-identifiable personal information that is no longer needed for a purpose permitted under the Unified Privacy Principles (UPPs). This guidance should cover among other things: (a) personal information that forms part of a historical record;	It is insufficient to merely *suggest* that OPC issue such guidelines. The OPC should be required by the Act to issue guidelines on the retention principle within one year.

ALRC PROPOSALS	APF SUBMISSION
(b) personal information, or a record of personal information, that may need to be preserved, in some form, for the purpose of future dispute resolution; and (c) the interaction between the UPPs and legislative records retention requirements.	We refer again to our general reservations about OPC Guidelines in our Introduction.
Proposal 25–6 The Office of the Privacy Commissioner should provide guidance about what is required of an agency or organisation to destroy or render noon-identifiable personal information, particularly when that information is held or stored in an electronic form.	As discussed before, it is insufficient to merely *suggest* that OPC issue such guidelines. The OPC should be required by the Act to issue guidelines on the retention principle within one year. We refer again to our general reservations about OPC Guidelines in our Introduction.
Ch 26 – Access and Correction	
Proposal 26–1 The proposed Unified Privacy Principles should contain a principle called 'Access and Correction' that: (a) sets out the requirement that apply to organisation in respect of personal information that is held by organisations; and (b) contains a note stating that the provisions dealing with access and correction of personal information held by agencies are located in a separate Part of the *Privacy Act*.	We accept the ALRC's arguments for dealing with access and correction separately for agencies (where the relationship with the FOI Act is crucial) and organisations. We support the inclusion in the UPPs of an access and correction principle (UPP 9) applying only to organisations. See proposal 26-6 for exception (a) UPP 6.1(e) should be amended to add a second sentence: 'The extent of the refusal must be proportionate to the significance of the negotiations'. UPP 6.1(g) should be amended to insert 'specifically' before 'authorised'. A Note should be added after UPP 6.1 to remind organisations that exception (i) requires the active involvement of an Australian enforcement body. The Note after UPP 9.2 should be replaced by one advising that 'The mere fact that some explanation may be necessary in order to

ALRC PROPOSALS	APF SUBMISSION
	understand information such as a score or algorithm result should not be taken as grounds for withholding information under 9.2.'.
Proposal 26–2 (a) The proposed 'Access and Correction' principle should provide that, where an organisation is not required to provide an individual with access to his or her personal information because of an exception to the general provisions granting a right of access, the organisation must take reasonable steps to reach an appropriate compromise, involving the use of a mutually agreed intermediary, that would allow for sufficient access to meet the needs of both parties. (b) The Office of the Privacy Commissioner should provide guidance about the meaning of 'reasonable steps' in this context, making clear, for instance, that an organisation need not take any steps where this would undermine a lawful reason denying a request for access in the first place.	We support the basic proposition in 26-2(a), but suggest that the qualification 'provided that would allow for sufficient access to meet the needs of both parties' could become an obstacle to compromise rather than facilitating it. It will often be the case that neither party will be satisfied by a compromise but this is no reason not to provide for it. UPP 9.3 should be amended to replace 'provided that would allow for sufficient access to meet the needs of both parties' with 'to allow for access to at least some of the information.' We suggest that the Privacy Commissioner be empowered to act as an intermediary either if the parties requested it or in the event that they are unable to agree on an alternative. UPP 9.3 should be amended to add 'In the absence of agreement, the Privacy Commissioner would be the intermediary.' The Privacy Commissioner should be empowered to act as an intermediary in the context of UPP 9.3. We support proposal 26-2 (b), subject to our general comments elsewhere on OPC guidance. The Office of the Privacy Commissioner should be expressly required to issue guidance to the effect that organisations should only claim any relevant exceptions (grounds for withholding) to the minimum extent necessary and that they should wherever possible provide as much of the information held as possible, even if this means selective editing or suppression of material subject to one of the exceptions.
Proposal 26– 3 The proposed 'Access and Correction' principle should provide that an organisation must respond within a reasonable time to a request from an individual for access to	We support the inclusion of UPP 9.4 but suggest that some binding benchmarks be provided on both response times and fees.

ALRC PROPOSALS	APF SUBMISSION
personal information held by the organisation. The Office of the Privacy Commissioner should provide guidance about the meaning of 'reasonable time' in this context.	Either Regulations or a binding Code should set benchmarks for response times and fees in relation to access and correction requests.
Proposal 26-4 The proposed 'Access and Correction' principle should provide that where, in accordance with this principle, an organisation has corrected personal information it holds about an individual, and the individual requests that the organisation notify any other entities to whom the personal information has already been disclosed prior to correction, the organisation must take reasonable steps to do so, provided such notification would be practicable in the circumstances.	Support. The ALRC should consider recommending a qualified obligation, in relation to personal information that has been disclosed to third parties, to notify past and present recipients of any significant data quality issues that come to notice after disclosure. Such an obligation could be located in UPP 7, UPP 9 or integrated with the proposed new data breach notification obligation wherever that is located.
Proposal 26–5 The proposed 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual that the individual wishes to have corrected or annotated, the individual should seek to establish that the personal information held by the organisation is, with reference to a purpose of collection permitted by the Unified Privacy Principles, not accurate, complete, up-to-date and relevant.	We submit that it is too onerous to place the entire burden of evidence on the individual seeking to make a correction. We suggest a qualified test. UPP 9.5 should be amended to read 'to establish on the balance of probabilities …' UPP 9.5 should be amended to read 'with reference to the purpose(s) for which the information was collected.' UPP 9.6 should specify that the obligation in relation to disputed information has to be performed in a way which ensures that any annotation is made available to any subsequent user of the disputed information. UPP 9.7 should be amended to add a second sentence: 'The reasons should specify which of the exceptions in UPP 9 apply.' The OPC should issue guidance on the application of this sub-principle The Privacy Commissioner should be required to issue guidance to the effect that correction can take the form of amendment, deletion or addition, as appropriate in the circumstances. The guidance should also advise that there are many situations where there is a

ALRC PROPOSALS	APF SUBMISSION
	legal requirement to keep an historical record of actual transactions, but that this should not prevent the correction of 'operational' records, leaving the original incorrect information only in an archive.
Proposal 26–6 The proposed 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual, it is not required to provide access to that information to the individual to the extent that providing access would be reasonable likely to pose a serious threat to the life of health of any individual.	Support – this is a specific application of the exception where we accept the case for the deletion of 'imminent'.
Ch 27 – Identifiers	
Proposal 27–1 The proposed Unified Pirvacy Principles should contain a principle labelled 'Identifiers' that applies to agencies and organisations. As a consequence, s 100(2) and (3) of the Privacy *Act* should be amended to apply also to agencies.	Support.
Proposal 27– 2 The proposed 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or any other particular that: (a) uniquely identifies an individual for the purpose of an agency's or organisation's operations; or (b) is determined to be an identifier by the Office of the Privacy Commissioner	Support. The definition of 'identifier' should also encompass when identifiers are used for authentication (verification) and not only when used for identification.
Proposal 27–3 The proposed 'Identifiers' principle should contain a note stating that 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)	Support. UPP 10.3 and UPP 10.4(d) should be deleted, and any exceptions left to the public interest determination process.
Proposal 27–4 The proposed 'Identifiers' principle should regulate the use by agencies and organisation of identifiers that are assigned by state and territory agencies.	Support.
Question 27–1 Should the *Privacy Act* regulate the assignment of identifiers by agencies, organisations or both? If so, what requirements should apply and should these requirements be located in the proposed Unified Privacy Principles or elsewhere?	
Proposal 27– 5 Before the introduction by agencies of any unique multi-purpose identifier, the	This allows for far too little public input or disclosure, and is liable

ALRC PROPOSALS	APF SUBMISSION
Australian Government should, in consultation with the Privacy Commissioner, consider the need for a privacy impact assessment.	to be both skewed by the terms of reference or choice of consultant to ensure that key questions are not asked, or hidden if the results are not to the government's liking, as recent examples have demonstrated (see our submission on PIAs generally in our response to Part F of DP 72). The Act should require that, before the introduction by agencies of any unique multi-purpose identifier, an independent and public privacy impact assessment should be commissioned, the terms of reference of which should be a determination by the Privacy Commissioner, such a determination being a legislative instrument. Any exceptions to UPP10 should be clearly set out in legislation. We agree with the ALRC's view that the number on the 'access card' proposed by the previous government would have been likely to fall within the definition of 'identifier' (DP72, [27.109]). So too would the underlying registration number, which would have been even more of a risk to privacy than the card number.
Proposal 27–6 The Office of the Privacy Commissioner, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the *Tax File Number Guidelines* issued under s 17 of the *Privacy Act*.	Support. The OPC should be required by the Act to review within one year the Tax file number (TFN) Guidelines (Rules) so as to make them consistent with UPP 10.
Ch 28 – Transborder Data Flows	
Proposal 28–1 The Privacy Act should be amended to apply to acts done or practices engaged in, outside Australia by an agency.	Support.
Proposal 28-2 The proposed Unified Privacy principles should contain a principle called 'Transborder Data Flows' that applies to agencies and organisations.	Support.
Proposal 28– 3 The proposed 'Transborder Data Flows' principle should provide that an agency or organisation in Australia or an external Territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia if the transfer is necessary for one or more of the following by or on behalf of	We defer to and endorse the to the submission on this proposal by the Cyberspace Law and Policy Centre

ALRC PROPOSALS	APF SUBMISSION
an enforcement body: (a) 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. (b) the enforcement of laws relating to the confiscation of the proceeds of crime; (c) the protection of the public revenue; (d) the prevention, detection, investigation or remedying of seriously improper conduct or proscribed conduct; (e) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; (f) extradition and mutual assistance.	
Question 28–1 Should the Privacy Act provide that for the purposes of the proposed "Transborder Data Flows' principle, a 'transfer': (a) includes where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia; (b) excludes the temporary transfer of personal information, such as when information is emailed from one person located in Australia to another person also located in Australia, but, because of internet routing, the email travels (without being viewed) outside Australia on the way to its recipient in Australia?	We defer to the submission on this question by the Cyberspace Law and Policy Centre. 'Transfer' should include where personal information is stored in Australia in such a way that allows it to be accessed or viewed outside Australia. However, the ALRC should consider whether as a result any additional exception allowing some transfers in non-business and non-government settings should be made. 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.
Proposal 28–4 Subject to Proposal 28–3, the proposed 'Transborder Data Flows' principle should provide that an agency or organisation in Australia or an external territory may transfer personal information about an individual to a recipient (other than the agency, organisation or the individual) who is	We note that the ALRC appears to have accepted without question that the transborder principle should, as NPP 9 does now, only apply to transfers to foreign countries/outside Australia (ALRC DP 72 [28.42-28.44]).

ALRC PROPOSALS	APF SUBMISSION
outside Australia only if at least one of the following conditions is met: (a) the agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the proposed UPPs; or (b) the individual consents to the transfer; or (c) the agency or organisation continues to be liable for any breaches of the proposed UPPs; and (i) the individual would reasonably expect the transfer, and the transfer is necessary for the performance of a contract between the individual and the agency or organisation; (ii) the individual would reasonably expect the transfer, and the transfer is necessary for the implementation of pre-contractual measures taken in response to the individual's request; (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the agency or organisation and a third party; (iv) all of the following apply: the transfer is for the benefit of the individual; it is impracticable to obtain the consent of the individual to that transfer; and if it were practicable to obtain such consent, the individual would be likely to give it; or (v) before the transfer has taken place, the agency or organisation has taken reasonable steps to ensure that the information will not be dealt with by the recipient of the information inconsistently with the proposed UPPs.	We believe that the 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 organisation or agency not have to satisfy one of the exceptions in UPP 11 in order to be able to transfer personal information to a State government agency? The ALRC notes (but without comment on the implications) that the WA, Victorian and NT privacy laws all contain a transborder data transfer principle that applies to transfers *outside their own jurisdiction*; i.e. including to other Australian States and Territories (ALRC DP 72 [28.33]). We suggest that the ALRC explains more clearly in its final report how UPP 11 relates to and interacts with UPP 5. Every overseas transfer must also be either a use (if internal to an organization or agency) or a disclosure (if to a third party) and the organisation or agency must therefore also satisfy UPP 5. The UPP 11 exceptions are an additional hurdle that must be crossed where an overseas transfer is involved. Given this relationship, why does UPP 11 need to replicate some of the UPP 5 exceptions? We highlight this issue where it arises in the context of the individual UPP 11 exceptions. UPP condition (b) should require that the individual 'expressly' consents to the transfer. UPP 3 should provide for the individual concerned to be given notice of the specific country or countries to which the data may be transferred. The consent exception (b) in UPP 11 should be conditional on (i) compliance with this aspect of UPP 3, and (ii) notice when obtaining express consent of the fact that the transferor will no longer be liable for any breaches. The consent exception should also be conditional upon the obligation in UPP 11 (d)(v).

ALRC PROPOSALS	APF SUBMISSION
	Any 'enforcement' exception to UPP11 must be more tightly worded and conditional.
Proposal 28–5 The proposed 'Use and Disclosure' principle should contain a note stating that agencies and organisation are subject to the requirements of the proposed "Transborder Data Flows' principle when transferring personal information about an individual to a recipient who is outside Australia.	Support
Proposal 28–6 The proposed 'Transborder Data Flows' principle should contain a note stating that agencies and organisations are subject to the requirement of the proposed 'Use and Disclosure' principle when transferring personal information about an individual to a recipient who is outside Australia.	Support
Proposal 28–7 Section 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia, this transfer will be subject to the proposed 'Transborder Data Flows' principle.	Support.
Proposal 28–8 The Australian Government should develop and publish a list of laws and binding schemes that effectively uphold principles for fair handling of personal information that are substantially similar to thee proposed Unified Privacy Principles.	We support the ALRC's proposal that there should be a 'whitelist' of such 'substantially similar' protections published Any 'whitelist' in relation to UPP 11(a) should be by a regulation or other legislative instrument made by the government, and made after receipt of published advice from the Privacy Commissioner. The proposed exception requires the overseas 'scheme' to '*effectively* uphold privacy protections…' (emphasis added). The ALRC argues that in these circumstances an individual can seek redress overseas. We suggest that this is unrealistic in that private individuals cannot be expected to have the necessary skills, knowledge and resources to do so successfully on their own. In our view it is essential that for a foreign scheme to be judged as eligible for the whitelist, there must be an agreement in place between the Privacy Commissioner and appropriate regulators in the other jurisdiction, to facilitate complaint investigation and cross-border enforcement. The Privacy Commissioner already has such an agreement with the NZ Privacy

ALRC PROPOSALS	APF SUBMISSION
	Commissioner, and similar arrangements are one of the priorities for implementation of the APEC Privacy Framework. In order to qualify for the 'whitelist' for the purposes of UPP 11(a), a foreign jurisdiction must have in place an agreement on cross border enforcement with the Australian Privacy Commissioner. In the ALRC's view, agencies and organisations should not remain accountable when they reasonably believe that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the proposed UPPs ([28.70]). In our view, in the absence of any such clear expression of public policy in the form of a 'whitelist' legislative instrument, there is no justification for privileging mere subjective belief of the data exporter by releasing them from all breaches of the UPPs which are subsequently committed by the overseas recipient or others. Why should the person whose privacy has been infringed be forced to take legal proceedings in a foreign jurisdiction? Instead, as we have argued previously, the exporter should remain liable, as in exception (d)(see our IP 31 submission 13-1). Except where a transfer is to a jurisdiction included in a 'whitelist' legislative instrument, the agency or organisation should continue to be liable for any breaches of the UPPs (as in exception (d)).
Proposal 28–9 The Office of the Privacy Commissioner should develop and publish guidance on the proposed 'Transborder Data Flow' principle, including guidance on: (a) when personal information may become available to a foreign government; (b) outsourcing government services to organisations outside Australia; (c) the issues that should be addressed as part of a contractual agreement with the overseas recipient of personal information;	Support, subject to our generic concerns about OPC guidance in our submission on Part F of ALRC DP 72. We support the ALRC's encouragement to the Australian Government and the OPC to continue to seek opportunities for further cooperation with privacy regulators outside Australia ([24.104]).

ALRC PROPOSALS	APF SUBMISSION
(d) when a transfer of personal information is 'for the benefit' or 'in the interests of' the individual concerned; and (e) what constitutes 'reasonable steps' to ensure the information it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the proposed Unified Privacy principles.	
Proposal 28–10 The Privacy Policy of an agency or organisation, referred to in the proposed 'Openness' principle, should set out whether personal information is likely to be transferred outside Australia.	Support - a requirement to notify would be one of the most effective protections against inappropriate transfers. It should extend to notification of *which* jurisdiction data is to be transferred, and the identity of the recipient in that jurisdiction. It will assist individuals to exercise informed choice and/or bring pressure to bear for improvements in legislative protection, at least in Australian jurisdictions without adequate laws. We have already argued above for this specific notification to be made a condition of the consent exception in UPP 11(b), and repeat the suggestion that is also be made a more generic requirement of UPP 3.
Question 28–2 Would trustmarks be an effective method of promoting compliance with, and reinforcement of, the *Privacy Act* and other international privacy regimes? If so should they be provided for under the *Privacy Act*?	Trustmarks should not be provided for in the Privacy Act, and OPC should not be involved with them except where there is a compelling case of value to consumers, and the involvement of consumer organisations in their operation.
Embedded question at 28.17 - Should the *Privacy Act* limit the circumstances when personal information transferred outside Australia will become subject to a foreign law?	See above
Embedded proposal at 28.19 - The ALRC proposes that the OPC develop and publish guidance on the proposed 'Transborder Data Flows' principle. This should set out the steps to be taken when personal information transferred outside Australia may become subject to foreign law, including laws such as the USA Patriot Act. The guidance should also provide advice to agencies when contracting government services to organisations outside Australia.	See above
Embedded proposal at 28.56 - To assist agencies and organisations make these assessments [for 'benefit of the individual'], the ALRC proposes that the OPC develop and publish guidance	We support these suggestions, subject to our general comments about OPC guidance (see our submission on ALRC DP 72 Part F).

ALRC PROPOSALS	APF SUBMISSION
on the proposed 'Transborder Data Flows' principle, which addresses when a transfer of personal information is for the benefit or in the interests of the individual concerned.	
Embedded question at 28.62 - Only one submission addressed the need for a provision dealing with exceptional or specified circumstances and did not specify what those circumstances should include.79 The ALRC is interested in hearing from other stakeholders about this issue.	
Embedded question at 28.69 - To what extent should agencies and organisations remain liable when transferring personal information overseas?	See above
Ch 29 – Additional Privacy Principles	
No proposals or questions	

DP72 Part E - Exemptions

ALRC PROPOSALS	APF SUBMISSION
PART E- Exemptions	
Ch 30 – Overview	
Proposal 30–1 The Privacy Act should be amended to group together in a separate part of the Act exemptions for certain categories of entities or types of acts and practices.	Support
Proposal 30-2 The Privacy Act should be amended to set out in a schedule to the Act exemptions for specific, named entities. The schedule should distinguish between entities that are completely exempt and those that are partially exempt from the Privacy Act. For those entities that are partially exempt, the schedule should specify those acts and practices that are exempt.	Support
	As a general principle, we believe that few if any agencies or organisations need to be wholly exempt from the obligation to comply with all privacy principles. The case for exemption usually relates to difficulties in balancing the effect of particular principles with other public or private interests. Wholly exempting any agency from all principles is a lazy way of dealing with specific issues. We cannot for example think of any reason why all agencies and organisations should not have to comply with the security principle – any difficulties are adequately addressed by the 'reasonable steps' qualification.
Ch 31 – Defence and Intelligence Agencies	
Proposal 31–1 The privacy rules and guidelines, which relate to the handling of intelligence information concerning Australian persons by the Australian Security Intelligence Organisation, Australian Security Intelligence Service, Defence Imagery and Geospatial Organisation, Defence Intelligence Organisation, Defence Signals Directorate and Office of National Assessments, should be amended to include consistent rules and guidelines relating to:	Support

ALRC PROPOSALS	APF SUBMISSION
(a) incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of the incident and measures taken to protect the privacy of the Australian person); (b) the accuracy of personal information; and (c) the storage and security of personal information.	
Proposal 31–2 Section 15 of the *Intelligence Services Act 2001* (Cth) should be amended to provide that: (a) the responsible minister in relation to the Defence Intelligence Organisation is required to make written rules regulating the communication and retention by the Defence Intelligence Organisation of intelligence information concerning Australian persons; and (b) before making rules to protect the privacy of Australian persons, the ministers responsible for the Australian Security Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate and the Defence Intelligence Organisation should consult with the Office of the Privacy Commissioner.	Support
Proposal 31–3 The *Office of National Assessments Act 1977* (Cth) should be amended to provide that: (a) the responsible minister in relation to the Office of National Assessments (ONA) is required to make written rules regulating the communication and retention by the ONA of intelligence information concerning Australian persons; and (b) before making rules to protect the privacy of Australian persons, the minister responsible for the ONA should consult with the Office of the Privacy Commissioner.	Support
Proposal 31–4 Section 8A of the *Australian Security and Intelligence Organisation Act 1979* (Cth) should be amended to provide that, before making rules to protect the privacy of Australian persons, the responsible minister should consult with the Office of the Privacy Commissioner.	Support

ALRC PROPOSALS	APF SUBMISSION
Proposal 31–5 The privacy rules and guidelines referred to in Proposal 31–1 should be made available electronically to the public; for example, on the websites of those agencies.	Support – but why not those under Proposals 31-2 to 31-4 as well?
Proposal 31–6 The Privacy Act should be amended to apply to the Inspector-General of Intelligence and Security (IGIS) in respect of the administrative operations of that office.	Support
Proposal 31–7 The Inspector-General of Intelligence and Security, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines to ensure that the personal information handled by IGIS is protected adequately.	Support
Ch 32 – Federal Courts and Tribunals	
Embedded Position: Exemption for Federal Courts - "In the ALRC's view, federal courts should continue to be exempt in respect of matters of a non-administrative nature" (32.22)	Support
Embedded Proposal: Non-Party Access to Court Records - The ALRC reaffirms its recommendation made in ALRC 98, that SCAG order a review of court and tribunal rules in relation to non-party access to court records, with a view to promoting a national and consistent policy (32.54)	Support
Proposal 32-1: Research Access Federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.	Support
Embedded Position: The ALRC does not consider that parties and witnesses to proceedings should have the right to change or annotate court records (ALRC 32-61)	
Embedded Question: Individual Right of Access - The ALRC is interested in views on whether any exceptions should apply when granting an individual the right to access his or her own personal information held by a federal tribunal (32.105).	
Question 32-1: Should the *Privacy Act* be amended to provide that federal tribunals are exempt from the operation of the Act in respect of their adjudicative functions? If so, what should be the scope of 'adjudicative functions'?	Federal tribunals appear to operate without major difficulties despite being subject to the IPPs. We see no need for any general exemption.

ALRC PROPOSALS	APF SUBMISSION
Ch 33 – Exempt Agencies under the *Freedom of Information Act 1982* (Cth)	
Proposal 33-1 The *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Fair Pay Commission under s 7(1) of the Act.	Support
Proposal 33-2 The following agencies listed in Schedule 2 Part I Division 1 and Part II Division 1 of the *Freedom of Information Act 1982* (Cth) should be required to demonstrate to the Attorney-General of Australia that they warrant exemption from the operation of the *Privacy Act*: (a) Aboriginal Land Councils and Land Trusts; (b) Auditor-General; (c) National Workplace Relations Consultative Council; (d) Department of the Treasury; (e) Reserve Bank of Australia; (f) Export and Finance Insurance Corporation; (g) Australian Communications and Media Authority; (h) Classification Board; (i) Classification Review Board; (j) Australian Trade Commission; and (k) National Health and Medical Research Council. The Australian Government should remove the exemption from the operation of the *Privacy Act* for any of these agencies that, within 12 months, do not make an adequate case for retaining their exempt status.	Support, but there must be a process of public consultation on any claims for exemption AUSTRAC should also have to justify any limited exemptions.
Proposal 33-3 The *Privacy Act* should be amended to remove the exemption of the Australian Broadcasting Corporation and the Special Broadcasting Service listed in Schedule 2 Part II	Support

ALRC PROPOSALS	APF SUBMISSION
Division 1 of the *Freedom of Information Act 1982* (Cth).	
Ch 34 – Other Public Sector Exemptions	
Proposal 34-1 The Attorney-General's Department, in consultation with the Office of the Privacy Commissioner, should develop and publish information handling guidelines for royal commissions to assist in ensuring that the personal information they handle is protected adequately.	Support
Proposal 34–2 The Privacy Act should be amended to remove the exemption that applies to the Australian Crime Commission and the Board of the Australian Crime Commission by repealing s7(1)(a)(iv), (h) and 7(2) of the Act.	Support
Proposal 34–3 The Privacy Act should be amended to apply to the Integrity Commissioner in respect of the administrative operations of his or her office.	Support
Proposal 34–4 The Integrity Commissioner, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines to ensure that the personal information handled by the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity is protected adequately.	Support
Question 34–1 Should the Privacy Act be amended to set out, in the form of an exemption, the range of circumstances in which agencies that perform law enforcement functions, such as the Australian Federal Police and the Australian Crime Commission, are not required to comply with specific privacy principles?	Yes, if any such exemptions can be justified, though a process of open public consultation (some information may need to be withheld on security grounds but there can be no justification for a wholly secret process).
Question 34–2 Should the Department of the Senate, the Department of the House of Representatives and the Department of Parliamentary Services continue to be exempt from the operation of the Privacy Act? If so, what should be the scope of the exemption?	No – these Departments should be required to justify any selective exemptions through an open consultative process.
Proposal 34–5 Subject to Proposal 4–4 (states and territories to enact legislation applying the proposed Unified Privacy Principles and Privacy (Health Information) Regulations), the Privacy Act should be amended to: (a) apply to all state and territory incorporated bodies, including statutory corporations, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of the relevant obligations in the Privacy Act; and (b) empower the Governor-General to make regulations exempting state and territory	Support

ALRC PROPOSALS	APF SUBMISSION
incorporated bodies from coverage of the Privacy Act on public interest grounds.	
Proposal 34–6 The Privacy Act should be amended to provide that, in considering whether to exempt state and territory incorporated bodies from coverage of the Privacy Act, the Minister must: (a) be satisfied that the state or territory has requested that the body be exempt from the Act; (b) consider: (i) whether coverage of the body under the Privacy Act adversely affects the state or territory government; (ii) the desirability of regulating under the Privacy Act the handling of personal information by that body; and (iii) whether the state or territory law regulates the handling of personal information by that body to a standard that is at least equivalent to the standard that would otherwise apply to the body under the Privacy Act; and (c) consult with the Privacy Commissioner about the mattersmentioned in paragraphs (ii) and (iii) above.	Support
Ch 35 – Small Business Exemption	
Proposal 35–1 The *Privacy Act* should be amended to remove the small business exemption by; (a) deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and (b) repealing ss 6D–6EA of the Act.	Support
Proposal 35–2 Before the proposed removal of the small business exemption from the *Privacy* Act comes into effect, the Office of the Privacy Commissioner should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by: (a) establishing a national small business hotline to assist small businesses in complying with the Act; (b) developing educational materials – including guidelines, information sheets, fact sheets and checklists – on the requirements under the Act; (c) developing and publishing templates for small businesses to assist in preparing Privacy Policies, to be available electronically and in hard copy free of charge; and	Support

ALRC PROPOSALS	APF SUBMISSION
(d) liaising with other Australian Government agencies, state and territory authorities and representative industry bodies to conduct programs to promote an understanding and accepting of the privacy principles.	
Ch 36 – Employee Records Exemption	
Proposal 36–1 The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.	Support
Proposal 36–2 The *Privacy Act* should be amended to provide that an agency or organisation may deny a request for access to evaluative material, disclosure of which would breach an obligation of confidence to the supplier of the information. 'Evaluative material' for these purposes means evaluative or opinion material compiled solely for the purpose of determining the suitability, eligibility or qualifications of the individual concerned for employment, appointment or the award of a contract, scholarship, honour, or other benefit.	Oppose – modern HR practice can and should accommodate openness of referee reports etc – UPP 6 has an exemption for 'intentions' and any FOI parts of the Act could do the same
Ch 37 – Political Exemption	
Proposal 37–1 The *Privacy Act* should be amended to remove the exemption for registered political parties and the exemption for political acts and practices by: (a) deleting the reference to a 'registered political party' from the definition of 'organisation' in s 6C(1) of the Act; (b) repealing s 7C of the Act; and (c) removing the partial exemption that is currently applicable to Australian Government ministers in s7(1) of the Act.	Support
Proposal 37–2 The *Privacy Act* should be amended to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication.	Support
Proposal 37-3 Before the proposed removal of the exemptions for registered political parties and for political acts and practices from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and	Support

ALRC PROPOSALS	APF SUBMISSION
others to assist them in understanding and fulfilling their obligations under the Act.	
Ch 38 – Media Exemption	
Proposal 38–1 The Privacy Act should be amended to define 'journalism' an the collection, preparation for (a) material having the character of news, current affairs or documentary; or (b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary.	Support
Proposal 38–2 In consultation with the Australian Communications and Media Authority and peak media representative bodies, the Office of the Privacy Commissioner should establish criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.	Support
Proposal 38-3 The Office of the Privacy Commissioner should issue guidelines containing the criteria for assessing the adequacy of media privacy standards established under Proposal 38–2.	These criteria are too important to be left to Guidelines – the Privacy Commissioner should be required to develop and publish binding rules.
Proposal 38-4 Section 7B(4)(b)(i) of the Privacy Act should be amended to provide that the standards must 'deal adequately with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters)'.	Support
Proposal 38–5 The Office of the Privacy Commissioner should issue guidance to clarify that that the term 'publicly committed' in s.7B(4) of the Privacy Act requires both: (a) express commitment by a media organisation to observe privacy standards that have been published in writing by the media organisation or a person or body representing a class of media organisations; and (b) conduct by the media organisation evidencing commitment to observe those standards.	Support, subject to the binding rules to be issued setting criteria for assessing the adequacy of media standards (see our response to Proposal 38-3) including an express requirement for adequate External Dispute Resolution mechanisms.
Ch 39 – Other Private Sector Exemptions	
No proposal or questions. However:	

ALRC PROPOSALS	APF SUBMISSION
(i) Related bodies corporate. At p.41 of the DP the ALRC states: "the OPC has suggested that an improved notice of disclosure by the relevant body corporate could ameliorate this concern. Currently, NPP 1.3(d) requires an organisation to take reasonable steps to ensure that an individual is aware of the organisations or types of organisations to which the information is usually disclosed. The ALRC does not consider that requiring a more detailed notice of disclosure—for example, one that lists all related companies by name—would adequately address concerns about direct marketing. A better alternative is to provide individuals with the means to opt out of direct marketing [addressed in ch. 23].	Disagree – greater transparency is needed – individuals cannot be expected to know or find out about complex corporate relationships. Listings of related companies by name do not need to be in every privacy notice but do need to be readily accessible, such as on a web site. Section 13B should be repealed. The Direct Marketing 'opt-out' to be provided under UPP 6 only addresses one particular type of potential privacy harm. There are many other potential harms for which individuals may need to trace a pattern of use and disclosure between related entities.
Ch 40 – New Exemptions	
Question 40–1 Should the Australian Government request that the Standing Committee of Attorney's-General consider the regulation of private investigators and the impact of federal, state and territory privacy and related laws on the industry?	We see no need for a review of privacy laws in relation to the activities of private investigators, who should remain subject to all of the principles. There may well be other reasons for such a review.
Question 40–2 Should the *Privacy Act* or other relevant legislation be amended to provide exemptions or exceptions applicable to the operation of alternative dispute resolution (ADR) schemes? Specifically, should the proposed: (a) 'Specific Notification' principle exempt or except ADR bodies from the requirement to inform an individual about the fact of collection of personal information, including unsolicited personal information, where to do so would produce an obligation of privacy owed to a party to the dispute, or could cause safety concerns for another individual; (b) 'Use and Disclosure' principle authorise the disclosure of personal and sensitive information to ADR bodies for the purpose of dispute resolution; and (c) 'Sensitive Information' principle authorise the collection of sensitive information without consent by an ADR body where necessary for the purpose of dispute resolution?	We accept that there may be difficulties in fully complying with all privacy principles in the course of dispute resolution, particularly in relation to personal information about third parties. We support a review of the application of privacy principles in the context of dispute resolution (both internal – IDR, and external (EDR)), with a view to justifying selective exemptions.

DP72 Part F – Office of the Privacy Commissioner

ALRC PROPOSALS	APF SUBMISSION
PART F – Office of the Privacy Commissioner	
Ch 41 – Overview	
No proposals or questions	
Ch 42 – Facilitating Compliance	
No proposals or questions	
Ch 43 – Office of the Privacy Commissioner	
	General Submission: There is significant community dissatisfaction with the way in which OPC has carried out its responsibilities throughout its 18 year existence. The information available about complaint outcomes reinforces this concern. The ALRC should ensure that these concerns are reflected in its final recommendations, as there is no point having an Act containing sound privacy principles if they are not being effectively enforced for the benefit of the community
Proposal 43-1 The *Privacy Act* should be amended to change the name of the "Office of the Privacy Commissioner' to the 'Australian Privacy Commission'.	Support
Proposal 43-2 Part IV, Division 1 of the *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. The Act should provide that, subject to the oversight of the Privacy Commissioner, the Deputy Commissioner may exercise all the powers, duties and functions of the Privacy Commissioner under this Act – including a power conferred by s 52 and a power in connection with the performance of the function of the Privacy Commissioner set out in s 28(1)(a) – of any other enactment.	In principle, we support the expansion of the OPC to include at least two statutory officers to provide additional support for changing the name of the OPC to the Australian Privacy Commission. We support the amendment of the Privacy Act to allow for the appointment of one or more Deputy Privacy Commissioners. The relationship between the Deputy Privacy Commissioner(s) and the Privacy Commissioner requires further clarification. The ALRC's view is that increasing the size of the OPC should facilitate more

ALRC PROPOSALS	APF SUBMISSION
	accountability and transparency in its operations and encourage more formal collegiate decision making (ALRC DP 72, [43.19]). We feel that more can be done in terms of facilitating more accountability and transparency. Multiple statutory officers may also facilitate greater functional separation to avoid a perceived conflict between the guidance and enforcement functions of the PC. However, this proposal will need to be reviewed in the context of the new political environment and already announced government plans – see our comments on this in the Introduction to this submission.
Proposal 43-3 Section 29 of the *Privacy Act* should be amended to provide that the Privacy Commissioner must have regard to the objects of the Act set out in Proposal 3-3 in the performance of his or her functions and the exercise of his or her powers.	Support (subject to our comments on the proposed objects in our submission on Part A)
Proposal 43-4 Section 82 of the *Privacy Act* should be amended to make the following changes in relation to the Privacy Advisory Committee: (a) require the appointment of a person to represent the health sector; (b) expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven; and (c) replace 'electronic data-processing' in S 82(7)(c) with 'information and communication technologies'.	Support
Proposal 43-5 The *Privacy Act* should be amended to empower the Privacy Commissioner to establish expert panels at his or her discretion to advise the Privacy Commissioner.	Support
Ch 44 – Powers of the Office of the Privacy Commissioner	
Proposal 44-1 The *Privacy Act* should be amended to delete the word 'computer' from s 27(1)(c) of the *Privacy Act.*	We support the ALRC's proposal to delete the word 'computer' from s 27(1)(c) of the *Privacy Act* in order to broaden the Commission(er)'s research and monitoring function to cover all technologies.

ALRC PROPOSALS	APF SUBMISSION
	The Commission(er)'s powers to report are unnecessarily constrained - in particular in those powers in s27 which only allow reports to be made to Ministers. The Commissioner should have an additional explicit power under s27 to report to the public, or to make a special report to the Parliament, on all of the matters listed in s27, excepting only those matters dealing with national security or involving equivalent considerations of confidentiality.
	The Commission(er) should have an additional duty, under s27, to provide to Parliament a document, to be tabled by the Minister on the next sitting day after receipt, wherever the Commission(er) considers that proposed legislation or regulations might significantly interfere with privacy, and stating whether such interferences would be justified or not in the Commissioner's view. This proposal may need to be reviewed in light of any statutory human rights charter, which would be likely to include a similar legislation review and assessment mechanism.
Proposal 44-2 The *Privacy Act* should be amended to reflect that where guidelines issued by the Privacy Commissioner are binding they should be renamed 'rules'. For example the following should be renamed to reflect that a breach of rules is an interference with privacy under s 13 of the *Privacy Act*: (a) Tax File Number Guidelines issued under s 17 of the *Privacy Act* should be renamed *Tax File Number Rules*; (b) Medicare and Pharmaceutical Benefits Programs Privacy guidelines (issued under s 135AA of the *National Health Act 1953*(Cth)) should be renamed the *Medicare and Pharmaceutical Benefits Programs Privacy Rules*; (c) Data-Matching Program (Assistance and Tax) Guidelines (issued under s 12 of the *Data-matching Program (Assistance and Tax) Act 1990*(Cth)) should be renamed the *Data-Matching Program (Assistance and Tax) Rules*; and (d) Guidelines for National Privacy Principles about genetic information should be renamed	Support – important to avoid semantic confusion about status of mere guidance vs binding rules. Note that elsewhere we make the case for more guidance being 'firmed up' in rules.

ALRC PROPOSALS	APF SUBMISSION
Genetic Information Privacy Rules.	
Proposal 44-3 Following the adoption of Proposal 19–1 to require agencies to produce and publish Privacy Policies, the *Privacy Act* should be amended to remove the requirement in s 27(1)(g) to maintain and publish the Personal Information Digest.	Oppose – despite lack of use to date Digest remains a potentially valuable resource and contribution to government openness and accountability. Now that the system of processing Digest returns is established there is little marginal cost in continuing it. The Commission(er) could facilitate increased use of the Digest with some enhancements in its internet publication.
Proposal 44-4 The Privacy Act should be amended to empower the Privacy Commissioner to: (a) direct an agency or organisation to provide to the Privacy Commissioner a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and (b) report to the Minister an agency or organisation's failure to comply with such a direction.	Strongly support, subject to our submission about reporting to the public.
Proposal 44-5 The Office of the Privacy Commissioner should develop Privacy Impact Assessment Guidelines tailored to the needs of organisations.	Support – these should be little different from existing guidelines for agencies – the recent publication of a PIA Handbook by the UK Information Commissioner should also provide valuable input.
Proposal 44-6 The *Privacy Act* should be amended to empower the Privacy Commissioner to conduct audits of the records of personal information maintained by organisation for the purpose of ascertain whether the records are maintained according to the proposed Unified Privacy Principles, Privacy Regulations, Rules and any privacy code that binds the organisation.	Support
Proposal 44-7 The Office of the Privacy Commissioner should maintain and publish on its website a list of all the Privacy Commissioner's functions, including those functions that arise under other legislation.	Support. In addition, all of the Commission(er)'s functions should be located or relocated, or if appropriate repeated, in the Privacy Act. Any other legislation to which a function relates should contain an explicit cross-reference to the Commission(er)'s role and the Privacy Act function
Proposal 44-8 The *Privacy Act* should be amended to empower the Privacy Commissioner to refuse to accept an application for a public interest determination where the Privacy	We are concerned that this would allow the Commission(er) to dismiss applications too readily. We endorse the submission from the

ALRC PROPOSALS	APF SUBMISSION
Commissioner is satisfied that the application is frivolous, vexatious, misconceived or lacking in merit.	Cyberspace Law and Policy Centre that this proposal be re-worded to read ‘‘…where the Commissioner is satisfied that the application is misconceived as to the purposes of public interest determinations, or so lacking in merit as not to be worthy of public consideration”
Proposal 44-9 Part IIIAA of the *Privacy Act* should be amended to specify that: (a) privacy codes approved under Part IIIAA operate in addition to the proposed Unified Privacy Principles (UPPs) and do not replace those principles; and (b) a privacy code may provide guidelines of standards on how any one or more of the proposed UPPs should be applied, or are to be complied with, by the organisation bound by the code, as long as such guidelines or standards contain obligations that are at least equivalent to those under the Act.	Support this change to the status and objective of Codes (but see our comments in our Introduction about the hierarchy of instruments and their status)
Proposal 44-10 Part IIIAA of the *Privacy Act* should be amended to empower the Privacy Commissioner to: (a) request the development of a privacy code to be approved by the Privacy Commissioner pursuant to s 18BB; and (b) develop and impose a privacy code that applies to designated agencies and organisations.	Support both proposals
Ch 45 – Investigation and Resolution of Privacy Complaints	
Proposal 45-1 Section 41(1) of the *Privacy Act* should be amended to provide that, in addition to existing powers not to investigate, the Commissioner may decide not to investigate, or nor to investigate further, an act or practice about which a complaint has been made under s 36, or which the Commissioner has accepted under s 40(1B), if the Commissioner is satisfied that: (a) the complainant has withdrawn the complaint; or (b) the complainant has not responded to the Commissioner for a specified period following	Support (a) and (b) but not (c) – given the track record of successive Commissioners having been too willing to dismiss complaints. They should not be given even greater discretion to do so. If (c) was added, then if a complaint was dismissed under this new ground, OPC should be required to give more detailed justification, and there must be a right of appeal from the dismissal decision.

ALRC PROPOSALS	APF SUBMISSION
a request by the Commissioner for a response in relation to the complaint; or (c) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.	
Proposal 45-2 The *Privacy Act* should be amended to empower the Privacy Commissioner to: (a) decline to investigate a complaint where the complaint is being handled by an approved external dispute resolution scheme; or (b) decline to investigate a complaint that would be more suitably handled by an approved external dispute resolution scheme, and to refer that complaint to the external dispute resolution scheme with a request for investigation.	Support but only if there is a right of appeal to the PC (or direct to a tribunal or court) from the decision of the EDR scheme (merits review)
Proposal 45-3 Section 99 of the *Privacy Act* should be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers, including a power conferred by section 52, in relation to complaint handling conferred on the Commissioner by the *Privacy Act*.	Support, provided there is no loss of remedies/sanctions available to referred complainants – this will require a process of assessment and approval and monitoring of alternate State or Territory complaint handling mechanisms, and also satisfactory reporting. (See also our submission on proposed UPP11).
Proposal 45-4 Section 27(1)(a) and (ab) of the *Privacy Act* should be amended to make it clear that the Privacy Commissioner's functions in relation to complaint handling include: (a) to receive complaints about an act or practice that may be an interference with the privacy of an individual; (b) to investigate the act or practice about which complaint has been made; and (c) where the Commissioner considers it appropriate to do so and at any stage after acceptance of the complaint, to endeavour, by conciliation, to effect a settlement of the matters that gave rise to the complaint or to make a determination in respect of the complaint under s 52.	Support
Proposal 45-5 The *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should give effect to the following: (a) If, at any stage after receiving the complaint, the Commissioner considers it reasonably	Support (a) subject to time limits Strongly support (b) – a right to a Determination, but must not limit this to where Commissioner decides conciliation has failed –

ALRC PROPOSALS	APF SUBMISSION
possible that the complaint may be conciliated successfully, he or she must make all reasonable attempts to conciliate the complaint. (b) Where, in the opinion of the Commissioner, all reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination. (c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.	otherwise OPC could continue to avoid making Determinations by using a variety of other grounds to close a complaint. Successive Commissioners have proved extraordinarily averse to making Determinations, and any proposals in this area need to take this into account, by providing as few excuses as possible that cannot be reviewed or otherwise challenged. An applicant should also have the right to require a determination under s52 wherever the Commissioner proposes to refuse to investigate, or further investigate, a complaint. In such cases, it should be sufficient for the Commissioner to state in a letter that the determination is dismissed under s52, giving the reasons for refusing to investigate as the reasons for dismissal. Support (c)
Proposal 45-6 Section 52 of the *Privacy Act* should be amended to empower the Privacy Commissioner to make an order in a determination that an agency or respondent must take specified action within a specified period for the purpose of ensuring compliance with the Act.	Strongly support – this has been a major weakness of the current regime – best illustrated by the Commissioner's Determinations 1-4 of 2004.
Proposal 45-7 The *Privacy Act* should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner under s 52 and the current review rights set out in s 61 should be repealed.	Strongly support. There must however also be a right of appeal from a Commissioner's decision to dismiss a complaint (see proposal 45-1).
Proposal 45-8 The Office of the Privacy Commissioner should prepare and publish a document setting out its complaint-handling policies and procedures.	Support We also strongly endorse the detailed submission by the Cyberspace Law & Policy Centre concerning improved reporting of complaint statistics and outcomes.
Proposal 45-9 Section 38B(2) of the *Privacy Act* should be amended to allow a class member to withdraw from a representative complaint at any time if the class member did not consent to be a class member.	Support. While there is no evidence of any problem in relation to representative complaints we would certainly not support named individuals being parties to a complaint against their will.

ALRC PROPOSALS	APF SUBMISSION
Proposal 45-10 Section 42 of the *Privacy Act* should be amended to empower the Privacy Commissioner to make preliminary enquires of third parties as well as respondent.	Support
Proposal 45-11 Section 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to an NPP complaint or a code complaint accepted under s 40(1B), and any other relevant person, to attend a compulsory conference.	Support (will be UPP or Code complaint if other ALRC proposals are implemented).
Proposal 45-12 Section 69(1) and (2) of the *Privacy Act* should be deleted, which would allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant.	Support
Proposal 45-13 The *Privacy Act* should be amended to provide that the Privacy Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties if: (a) the Privacy Commissioner considers that the matter could be determined fairly on the basis of written submission from the parties; and (b) the complainant and the respondent consent to the matter being determined without oral submissions.	Support
Ch 46 – Enforcement (Enforcing the Privacy Act)	
Proposal 46-1 The *Privacy Act* should be amended to empower the Privacy Commissioner to: (a) issue a notice to comply to an agency or organisation following an own motion investigation, where the Commissioner determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual; (b) prescribe in the notice that an agency or respondent must take specified action within a specified period for the purpose of ensuring compliance with the Privacy Act; and (c) commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.	Support In addition, own motion investigations should be the subject of public notice by the Commissioner, and should have procedures developed for appropriate intervention by other interested parties (such as NGOs in the relevant area). As we have already suggested above, the Commissioner should be able to make a special report to Parliament of the results of an own motion investigation.
Proposal 46-2 The *Privacy Act* should be amended to allow a civil penalty to be imposed where there is a serious or repeated interference with the privacy of an individual. The Office	Strongly support

ALRC PROPOSALS	APF SUBMISSION
of the Privacy commissioner should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty is made.	
Ch 47 – Data breach notification	
Proposal 47-1 The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows: (a) an agency or organisation is required to notify the Privacy Commissioner and any affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised personal and the agency, organisation or the Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individuals. (b) An agency or organisation is not required to notify any affected individual where: (i) the specified information was adequately encrypted; (ii) the specified information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the proposed Unified Privacy Principles (provided that the personal information is not used or subject to further unauthorised disclosure); or (iii) the Privacy Commissioner does not consider that notification would be in the public interest. (c) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.	Strongly support all elements of this proposed obligation, but suggest that it be made either part of UPP 8 (Security) or a separate UPP. It is desirable that all the principal obligations on agencies and organisations be located in the one set of principles.

DP72 Part G – Credit reporting provisions

ALRC PROPOSALS	APF SUBMISSION
PART G—Credit Reporting Provisions	
Ch 48 – Overview—Credit Reporting	
No Proposals	At the outset, we challenge the industry view that Pt IIIA and the current Code are, overall, *more* onerous than the NPPs – they are more correctly seen as conditions for a licenced breach of NPPs, in that Part IIIA of the Act gives statutory backing for a form of bundled consent – in effect a mandatory centralised credit information system. We believe this should be expressly acknowledged in the ALRC final report, as it changes the perspective from which the different obligations are viewed.
Ch 49 – The Credit Reporting Provisions	
No Proposals	
Ch 50 – The Approach to Reform	
Proposal 50–1 The credit reporting provisions of the Privacy Act should be repealed and credit reporting regulated under the general provisions of the Privacy Act and proposed Unified Privacy Principles (UPPs).	Support In relation to the regulatory framework for credit reporting, we endorse the main findings and recommendations of the report by Galexia for Veda Advantage which we understand has been provided to the ALRC as a submission.
Proposal 50–2 Privacy rules, which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information, should be promulgated in regulations under the Privacy Act—the proposed Privacy (Credit Reporting Information) Regulations.	Support – draft Regulations must however be available for debate at the same time as the amendments repealing Part IIIA

ALRC PROPOSALS	APF SUBMISSION
Proposal 50–3 The obligations imposed on credit reporting agencies and credit providers by the proposed Privacy (Credit Reporting Information) Regulations should be in addition to those imposed by the UPPs.	Support
Proposal 50–4 The proposed Privacy (Credit Reporting Information) Regulations should be drafted to contain only those requirements that are different or more specific than provided for in the proposed UPPs.	Support
Proposal 50–5 The proposed *Privacy (Credit Reporting Information) Regulations* should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'.	We maintain our view that the proposed Regulations should continue to regulate a wider category of creditworthiness information (as s.18N does now).
Proposal 50–6 The definition of a 'credit reporting business' in the proposed *Privacy (Credit Reporting Information) Regulations*, if based on that in s 6(1) of the *Privacy Act*, should exclude the phrase 'other than records in which the only personal information relating to individuals is publicly available information'.	Support subject to clarification of relationship to Proposal 52-6
Proposal 50–7 The proposed *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the *Privacy Act* (whether by operation of s 11B of the *Privacy Act* or pursuant to determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.	Support in principle but there is a need to review existing classes of credit provider determinations made by the Commisisoner – not simply accept status quo
Question 50–1 Should organisations be regarded as credit providers if they make loans in respect of the provision of goods or services on terms that allow the deferral of payment, in full or in part, for at least thirty days as compared to seven days, as is currently the case under the OPC's *Credit Provider Determination No. 2006–4 (Classes of Credit Provider)*?	Yes – only 30 days or more.
Question 50–2 Should the definition of 'credit provider' under the *Credit Reporting Privacy Code 2004* (NZ) be adopted as the definition of 'credit provider' under the proposed *Privacy (Credit Reporting Information) Regulations*? That is, should 'credit provider' be defined simply as 'a person that carries on a business involving the provision of credit to an individual'; and	No – the NZ definition is far too broad – it is important that the Regulations continue to exclude businesses such as car hire and real estate, and employers.

ALRC PROPOSALS	APF SUBMISSION
credit as 'property or services acquired before payment, and money on loan'?	
Proposal 50–8 The proposed *Privacy (Credit Reporting Information) Regulations* should exclude: the reporting of personal information about foreign credit and foreign credit providers; and the disclosure of credit reporting information to foreign credit providers.	Support
Proposal 50–9 The Australian Government should consider including credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).	Support, but this should not be seen as another opportunity for business interests to argue for relaxation of the rules, but only as a way of avoiding any unneccesary inconsistencies.
Proposal 50–10 The proposed *Privacy (Credit Reporting Information) Regulations* should apply to personal information relating to credit advanced to an individual for any purpose and not limited to 'domestic, family or household' purposes as is currently the case under the definition of 'credit' in the *Privacy Act*.	Support
Proposal 50–11 Credit reporting agencies and credit providers should develop, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, an industry code dealing with operational matters such as default reporting obligations and protocols and procedures for the auditing of credit reporting information.	Support but depends on definition of 'operational matters' – APF would see some matters that industry regards as 'operational' as more fundamental and would want some of these in Regulations or binding Code/Rules.
Ch 51 – More Comprehensive Credit Reporting	
Proposal 51–1 The proposed *Privacy (Credit Reporting Information) Regulations* should permit the inclusion in credit reporting files of the following categories of personal information in addition to those currently permitted under s 18E of the *Privacy Act*: (a) the type of each current credit account opened (for example, mortgage; personal loan; credit card); (b) the date on which each current credit account was opened; (c) the limit of each current credit account (for example, initial advance, amount of credit approved, approved limit); and (d) the date on which each credit account was closed.	Oppose – no convincing evidence has been produced to support the claim that more information would be used to lend more responsibly rather than to increase the total amount of lending. In absence of better regulation of lending practices, (and especially in current economic environment), the Australian community cannot take the risk that more comprehensive credit reporting would not be used irresponsibly, with the potential for significant harm not only to individuals but also to the overall economy.

ALRC PROPOSALS	APF SUBMISSION
Proposal 51–2 The credit reporting industry code (see Proposal 50-11) should provide for access to information on credit information files according to principles of reciprocity. That is, in general, credit providers only should have access to the same categories of personal information that they provide to the credit reporting agency.	The ALRC should remain neutral on issue of reciprocity. It should instead endorse principles of 'tiered access' and separate justification for 'input to' and 'output from' credit reference databases.
Proposal 51–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for a review after five years of operation. The review should focus on the impact of more comprehensive credit reporting on privacy and the credit market.	Support a review in principle but it must be independent, and we suggest 3 years would be preferable.
Ch 52 – Collection of Credit Reporting Information	
Proposal 52–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the recording, on the initiative of the relevant individual, of information that the individual has been the subject of identity theft.	Support – but also need to mandate an obligation to take the record into account in automated credit systems. Should also not just be on request, but whenever a credit provider or credit reporting agency becomes aware - they should also be required to notify the individual) (see also our comments on the proposed data breach notification obligation in our submission on Part F (Chpt 47))
[52.25] (Invitation for comment) 'The ALRC would welcome further comment on the role of inquiry information under the more comprehensive credit reporting scheme proposed by it [Proposals 51-1, 2 and 3] and whether any other reform relating to the collection, use or disclosure of inquiry information is desirable'.	See our other responses
Proposal 52–2 Credit reporting agencies should only be permitted to list overdue payments of more than a minimum amount.	Support
Question 52–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide a minimum amount for overdue payments listed by credit reporting agencies? If not, by what mechanism should a minimum amount for overdue payments be set and enforced?	Yes – APF endorses the submissions from financial counselling NGOs suggesting a $200 threshold.
Proposal 52–3 The proposed *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques, as currently permitted under s 18E(1)(b)(vii) of the *Privacy Act*.	Support
Proposal 52–4 The proposed *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the	Support

ALRC PROPOSALS	APF SUBMISSION
National Personal Insolvency Index (NPII) administered under the *Bankruptcy Regulations 1966* (Cth).	
Proposal 52–5 Credit reporting agencies, in accordance with obligations to ensure the accuracy and completeness of credit reporting information, should ensure that credit reports adequately differentiate the forms of administration identified on the NPII.	Support
Question 52–2 Should the proposed *Privacy (Credit Reporting Information) Regulations* allow for the listing of a 'serious credit infringement' or similar and, if so, how should this concept be defined?	Yes but delete current (c) from s.18E(1)(b)(x) or its replacement in the Regulations – 'reasonable suspicion' is too subjective. Permission to list SCI should be contingent on membership of approved EDR scheme (see proposal 55-6)
Proposal 52–6 The proposed *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include publicly available information.	Support allowing for this, but it should not be mandatory. Also, publicly available information, whether held in credit information files or separately, should be regulated by the credit reporting Regulations if and when it is brought together with other information for the purposes of a credit report.
Proposal 52–7 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as that term is defined in s 6(1) of the *Privacy Act*.	Support, and should also ensure that the Regulations do not allow inclusion of information about 'lifestyle,'character or reputation' (currently prohibited by s18E(2)(f).
Proposal 52–8 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information about individuals the credit provider or credit reporting agency knows to be under the age of 18 years.	Support
Proposal 52–9 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that, at or before the time credit reporting information is collected about an individual, credit providers must take reasonable steps to ensure that the individual is aware of: (a) the fact and circumstances of collection (for example, how and where the information was collected); (b) the credit provider's and credit reporting agency's identity and contact details; (c) the fact that the individual is able to gain access to the information;	Support the content of this awareness obligation but it is still too ambiguous as to timing – it doesn't address contentious interpretation by the OPC which has allowed notice to be given at the time of a default listing by an assignee, even though there has been no initial notice.

ALRC PROPOSALS	APF SUBMISSION
(d) the main consequences of not providing the information; (e) the types of people, organisations, agencies or other entities to whom the credit provider and credit reporting agency usually discloses credit reporting information; and (f) the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her credit reporting information.	
Proposal 52–10 The proposed *Privacy (Credit Reporting Information) Regulations* should prescribe the specific circumstances in which a credit provider must inform an individual that personal information might be disclosed to a credit reporting agency, for example, in circumstances where the individual defaults in making payments.	Support, but the timing must be clearer than the current obligation – notice is too late to give the individual real choices if it is left until they default
Question 52–3 In what specific circumstances should a credit provider be obliged to inform an individual that personal information might be disclosed to a credit reporting agency; and what information should notices contain? Who should give notice when a debt is assigned—the original credit provider, the assignee or both?	Notification should be at all relevant times and by all relevant parties – duplication doesn't matter
Question 52–4 Should the proposed *Privacy (Credit Reporting Information) Regulations* prescribe specific circumstances in which a credit reporting agency must inform an individual that it has collected personal information?	Yes – The Regulations should prescribe the circumstances and at the same time answer Q 52-3
Ch 53 – Use and Disclosure of Credit Reporting Information	
Proposal 53–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information, based on those uses and disclosures currently permitted under ss 18K, 18L and 18N of the *Privacy Act*.	Support the Regulations listing permitted uses and disclosures
Proposal 53–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that, in addition, a credit reporting agency or credit provider may use or disclose credit reporting information for related secondary purposes, as permitted by the proposed 'Use and Disclosure' principle.	Strongly oppose – allowing related purpose defeats object of more prescriptive credit reporting Rules
Question 53–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* allow credit providers (but not credit reporting agencies) to disclose an individual's credit reporting	Yes – but access must only be indirect, via the credit provider.

ALRC PROPOSALS	APF SUBMISSION
information to a mortgage or trade insurer, where access to the information is required to assist in the assessment of the individual's credit worthiness?	
Proposal 53–3 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing.	APF supports the prohibition on the use or disclosure of credit reporting information for direct marketing.
Question 53–2 Should credit providers be permitted to use credit reporting information to 'pre-screen' credit offers? If so, should credit providers be required to allow individuals to opt out, or should credit providers only be permitted to engage in pre-screening if the individual in question has expressly opted in to receiving credit offers?	No – it is impossible to prevent this being used to circumvent the ban on direct marketing, and/or to avoid the important constraint that credit reporting information can only be accessed in relation to an actual application for credit
Question 53–3 If the use and disclosure of credit reporting information for identity verification purposes is not authorised under the proposed *Privacy (Credit Reporting Information) Regulations*, what other sources of data might be used by credit providers to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) and similar legislation? What are the advantages and disadvantages of the alternate sources of data?	APF opposes the use of credit reporting information for AML-CTF verification – the government expressly chose not to provide for this in AML-CTF Act. Changes to Privacy Act should not be made to allow this 'back door' access. Credit providers should have to rely on same sources for verification as all other reporting entities
Proposal 53–4 There should be no equivalent in the proposed *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information related to credit worthiness. The use and disclosure limitations should apply only to personal information maintained by credit reporting agencies and used in credit reporting.	Oppose – see Proposal 50-5 The Second reading speech for the credit reporting amendments clearly intended broader coverage of credit-worthiness information.
Suggestion not translated into a proposal - that the drafting of the Regulations consider if notification should replace consent (DP72, [53.116])	The ALRC should recommend that before the Regulations are drafted, further consultations take place as to whether some of the consent requirements be replaced with notification requirements.
Ch 54 – Data Quality and Security	
The ALRC suggests that matters such as time limits for listing defaults, and multiple listing, should be left to an Industry Code (ALRC DP 72 [54.17 to 54.26])	We favour mandatory binding provisions relating to these matters and endorse the submission from the Cyberspace Law & Policy Centre that they be addressed in the Regulations.

ALRC PROPOSALS	APF SUBMISSION
Proposal 54–1 The proposed *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a State or a Territory from bringing proceedings against the individual to recover the amount of the overdue payment.	Support
Proposal 54–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt, such as by entering into a scheme of arrangement with the credit provider, an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information file for the full five year period permissible under the regulations.	Support, provided 'new arrangement' is clearly defined
Proposal 54–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must: (a) enter into agreements with credit providers that contain obligations to ensure data quality in the information credit providers provide to credit reporting agencies; (b) establish and maintain controls to ensure that only information that is accurate, complete, up-to-date and relevant is used or disclosed; (c) monitor data quality and audit compliance with the agreements and controls; and (d) identify and investigate possible breaches of the agreements and controls.	Support
Proposal 54–4 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers and credit reporting agencies have an obligation to take reasonable steps to ensure that credit reporting information is accurate, up-to-date, complete and not misleading.	Support but add ' and relevant' (see UPP 7) We support the suggestion by the Consumer Action law centre that there should be an obligation on credit providers and credit reporting agencies to report systemic data quality problems, similar to obligations in other areas of financial regulation.
Proposal 54–5 The credit reporting industry code (see Proposal 50-11) should promote data quality by mandating procedures to ensure consistency and accuracy in the reporting of overdue payments and other personal information by credit providers. These procedures should deal with matters including:	Support in principle subject to our preference for more of these details being in the Regulations or a binding Code, as opposed to a purely 'advisory' code There should be a legislated maximum period

ALRC PROPOSALS	APF SUBMISSION
(a) the timeliness of the reporting of personal information, such as overdue payments; (b) the calculation of overdue payments for credit reporting purposes; (c) obligations to prevent the multiple listing of the same debt; (d) the updating of personal information reported, including where schemes of arrangement have been entered into; and (e) the linking of credit reporting information where it is unclear whether the information relates to more than one individual with similar identifying details or to one individual who has used different identifying details.	
Proposal 54–6 The proposed review of the *Privacy (Credit Reporting Information) Regulations* after five years' of operation (Proposal 51-3) also should consider whether further regulation is required to ensure the data quality of credit reporting information.	Support review but should be 3 years
Proposal 54–7 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.	Support location in Regulations but the periods should be re-justified, not just carried over.
Proposal 54–8 The proposed *Privacy (Credit Reporting Information) Regulations* should provide for the deletion of information about voluntary arrangements with creditors under Part IX and Part X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.	Support
Proposal 54–9 The proposed *Privacy (Credit Reporting Information) Regulations* should contain no equivalent to s 18G(b) and (c), dealing with the security of credit information files and credit reports, as these obligations are adequately covered by the proposed 'Data Security' principle.	Support
Ch 55 – Rights of Access, Complaint Handling and Penalties	
Question 55–1 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide that individuals have the right to obtain a free copy of their credit reporting information?	Yes

ALRC PROPOSALS	APF SUBMISSION
Question 55–2 Should the proposed *Privacy (Credit Reporting Information) Regulations* provide an equivalent to s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised by a person authorised in writing and for a credit-related purpose?	Need to provide for genuine 'authorities' but prevent coerced access – this is a difficult generic issue on which we comment in our other submissions.
Proposal 55–1 The proposed *Privacy (Credit Reporting Information) Regulations* should provide individuals with rights to access and correct credit reporting information based on the provisions currently set out in sections 18H and 18J of the *Privacy Act*.	Support, but need to mandate use of 'annotations' in automated credit systems – we understand that current systems do not recognise annotations which are therefore rendered ineffective as a safeguard.
Proposal 55–2 The proposed *Privacy (Credit Reporting Information) Regulations* should provide individuals with rights to be notified where a credit provider refuses an application for credit based wholly or partly on credit reporting information, based on the provisions currently set out in s 18M of the *Privacy Act*.	Support
Proposal 55–3 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include any credit score or ranking used by the credit provider, together with explanatory material on scoring systems, to allow individuals to understand how the risk of the credit application was assessed.	Support
Proposal 55–4 The proposed Privacy (Credit Reporting Information) Regulations should provide that: (a) credit reporting agencies and credit providers must handle credit reporting complaints in a fair, efficient and timely manner; (b) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint; (c) a credit reporting agency should refer to a credit provider for resolution of a complaint about the content of credit reporting information provided to the agency by that credit provider; and (d) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint it must immediately inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute	Support

ALRC PROPOSALS	APF SUBMISSION
resolution scheme or to the Privacy Commissioner.	
Proposal 55–5 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.	Support, subject to the need to improve the operation of the complaint handling mechanisms, on which we have already commented.
Proposal 55–6 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers may only list overdue payment information where the credit provider is a member of an external dispute resolution scheme approved by the Office of the Privacy Commissioner.	Support
Proposal 55–7 The proposed *Privacy (Credit Reporting Information) Regulations* should provide that credit providers have an obligation to provide evidence to individuals and dispute resolution bodies to substantiate disputed credit reporting information, such as default listings, and that if the information is not provided within 30 days the credit reporting agency must delete the information on the request of the individual concerned.	Support, subject to clear specification o when the 'clock' starts – preferably the date the dispute is notified to the credit reporting agency. The proposed industry code should address the issue of what happens to the listing during the 30 day challenge period
Proposal 55–8 The *Privacy Act* should be amended to: (a) remove the credit reporting offences by repealing ss 18C(4), 18D(4), 18K(4), 18L(2), 18N(2), 18R(2), 18S(3) and 18T; and (b) allow a civil penalty to be imposed where there is a serious or repeated breach of the proposed *Privacy (Credit Reporting Information) Regulations*.	Support

DP72 Part H – Health Services and Research

[Submission on Chapters 56 & 57 – Health Services – to follow]

DP 72 Chapter 58 - Health Research

> **Proposal 58-1** The Privacy Commissioner should issue one set of rules under the proposed exceptions to the 'Collection' principle and the 'Use and Disclosure' principle in the Unified Privacy Principles (UPPs) to replace the Guidelines Under Section 95 of the Privacy Act 1988 and the Guidelines Approved Under Section 95A of the Privacy Act 1988.

Submission: APF does not have any in-principle objection to Proposal 58-1 to streamline these provisions by bringing them under one set of guidelines, provided that the single set of rules clarifies, but does not weaken the current standards that exist

> **Proposal 58-2** The Privacy Act should be amended to extend the existing arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

APF notes the ALRC's discussion on this issue. We also note that the current 'National Statement on Ethical Human Research' applies more broadly to human research generally, rather than only health and medical research. We also note that there is other research of considerable importance outside the health area, and that there is often overlap between health and non-health research. However, APF has concerns that leaving the way open for personal data to be used for all types of human research under this provision may be too broad. We understand that the rules proposed in Proposal 58-1 and Human Research Ethics Committee (HREC) arrangements would apply, however, there may be situations where personal data is used for research that falls way outside public expectations on use of data for research purposes.

Submission: The APF would only support Proposal 58-2 for the extension of the research provisions in the Act to 'human research' if the current privacy standards apply. In particular, APF's support for this proposal is conditional upon the current 'public interest' test continuing to apply, rather than the weaker version proposed in Proposal 58-4 (see submissions on Proposal 58-4).

> **Proposal 58-3** The Privacy Act should be amended to provide that 'research' is any activity, including the compilation or analysis of statistics, subject to review by a Human Research Ethics Committee under the National Statement on Ethical Conduct in Human Research (2007).

Submission: APF supports Proposal 58-3. We support the suggestion in PIAC's submission about the possible creation of a 'default' Human Research Ethics Committee in each state and territory to deal with human research proposals from entities that do not have sufficient capacity or need to maintain a standing committee of this sort.

> **Proposal 58-4** The research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle should provide that before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the proposed UPPs.

Submission: APF opposes Proposal 58-4. The existing arrangements require that the public interest in the research must 'substantially' outweigh the public interest in maintaining the level of privacy protection. APF submits that this original requirement should be retained. This, together with the other provisions for Collection, Use and Disclosure in the Act, should provide sufficient support and flexibility for research activity.

It must be noted, that as research activity often involves highly sensitive data, there is a potential for harm or embarrassment where the information is used or disclosed without the consent of the individual. In the case of health and medical research, there may be serious individual and public health repercussions if individuals do not feel that their information is handled with appropriate privacy protections in place as they may be hesitant to seek medical help in future. In such cases, the 'public interest' in maintaining a high level of privacy protection involves taking into account any potential detrimental public health outcomes as well as potential consequences for the individual involved.

> **Proposal 58-5** The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, to ensure that the approaches adopted in the rules and the National Statement on Ethical Conduct in Human Research (2007) are compatible.

Submission: APF supports Proposal 58-5. Though we would also state that from the outset, achieving 'compatibility' must mean doing so while maintaining the existing privacy protections – these must not be diminished for the sake of compatibility.

> **Proposal 58-6** The National Statement on Ethical Conduct in Human Research (2007) should be amended to require that, where a research proposal seeks to rely on the research exceptions in the Privacy Act, it must be reviewed and approved by a Human Research Ethics Committee.

Submission: APF supports Proposal 58-6.

> **Proposal 58-7** In developing the rules to be issued in relation to research under the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle, the Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements currently imposed on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the Privacy Act, have clear goals and impose the minimum possible administrative burden to achieve those goals.

Submission: APF supports Proposal 58-7.

> **Proposal 58–8** The research exception to the proposed 'Collection' principle should state that, despite subclause 2.6, an agency or organisation may collect sensitive information about an individual where:
>
> (a) the collection is necessary for research;
> (b) the purpose cannot be served by the collection of information that does not identify the individual;
> (c) it is impracticable for the agency or organisation to seek the individual's consent to the collection;
> (d) a Human Research Ethics Committee 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 UPPs; and
> (e) the information is collected in accordance with rules issued by the Privacy Commissioner.
>
> Where an agency or organisation collects sensitive information about an individual in accordance with this provision, 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.

Submission: In principle APF supports subclauses (a), (b) (c) & (e) in proposal 58-8. However, note our comments on Proposal 58-4 relating to subclause (d) – APF only supports the extension to broader types of research on the condition that 'substantially outweighs' version of the public interest test is retained, rather than the proposed weaker version of 'outweighs'.
APF also recommends that this exception be worded to ensure that it is clear that all conditions (a) to (e) must be met. At present it is easy to miss the 'and' at the end of subclause (d). The exception could be worded "… despite subclause 2.6, an agency or organisation may collect sensitive information about an individual where all of the following conditions are met:"

> **Proposal 58–9** The research exception to the proposed 'Use and Disclosure' principle should state that despite the other provisions of the Use and Disclosure principle, an agency or organisation may use or disclose personal information where:
>
> (a) the use or disclosure is necessary for research;
> (b) it is impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;
> (c) a Human Research Ethics Committee 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 UPPs;
> (d) the information is used or disclosed in accordance with rules issued by the Privacy Commissioner; and
> (e) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the personal information in a form that would identify the individual or from which the individual would be reasonably identifiable.

Submission: In principle APF supports subclauses (a), (b) & (d) in proposal 58-9. However, note our comments on Proposal 58-4 relating to subclause (c) – APF only supports the extension to broader types of research on the condition that 'substantially outweighs' version of the public interest test is retained, rather than the proposed weaker version of 'outweighs'.

In relation to subclause (e), APF is concerned that the wording is inherently contradictory. If an organisation is disclosing 'personal information', then this implies that it is information that would allow a person to be identified. The original wording in the Act was that, in the case of disclosure, the organisation must reasonably believe that the recipient of the health information will not disclose the health information or personal information derived from the health information. If the research provisions are to be extended to non-health research, then this subclause should simply be amended to state that the agency or organisation must believe that the receiving organisation will not disclose the personal information.

APF also recommends that this exception be worded to ensure that it is clear that all conditions (a) to (e) must be met. At present it is easy to miss the 'and' at the end of subclause (d). The exception could be worded "…an agency or organisation may use or disclose personal information where all of the following conditions are met:"

> **Proposal 58-10** The Privacy Commissioner should provide guidance on the meaning of 'not reasonably identifiable'.

The approach suggested by the ALRC in Proposal 58-10 appears to conflate the meaning of 'not reasonably identifiable' data with 'non-identifiable data', and furthermore that this is subset of data that is essentially not covered by the provisions of the Act. This must be borne in mind in any further exploration of this proposal.

The APF supports further exploration of this issue, particularly if it helps to ensure that a very narrow approach to what is considered 'not reasonable' be applied. There is a risk that agencies and organisations may decide on a loose interpretation of this term, and on this basis apply a range of privacy invasive measures to data that in actual fact could be potentially identifiably, even if with significant effort. Therefore, as an example, even if significant effort is required to identify

individuals from a dataset, this in itself should not mean the data is 'not reasonably identifiable', as many organisations and agencies have the capacity, and often use this capacity, to make a significant effort to identify individuals from a dataset where the identity of individuals is not immediately apparent.

One major concern is that, due to technical advances, it is becoming easier to re-identify information contained in large databases even when this information has been partially or fully de-identified. This means that data that was once considered 'non-identifiable' now may be able to be re-identified using new data management techniques together with newly established datasets. APF is concerned that in establishing a category of 'not reasonably identifiable' data, the onus is removed from agencies and organisations to make data non-identifiable in an environment where in fact they need to work harder to ensure that data is really 'non-identifiable'.

Before guidance can be developed on the meaning of 'not reasonably identifiable', further research is needed to establish what practices are in place to ensure that data can be made 'non identifiable'.

Submission: Any guidance developed on the meaning of 'not reasonably identifiable' needs to (a) strongly recommend data be non-identifiable wherever possible, and (b) include strict review requirements so that the practical and technological implications of changes in this area can be fully assessed. We refer also to our general concerns about 'guidance' outlined in the Introduction to our submission, and in particular to the need for adequate consultation with all relevant stakeholders when developing guidance materials.

> **Proposal 58–11** The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:
>
> (a) the process by which a Human Research Ethics Committee should review a proposal to establish a health information database or register for research purposes;
>
> (b) the matters a Human Research Ethics Committee should take into account in considering whether the public interest in establishing the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and
>
> (c) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

Submission: APF supports Proposal 58-11, on condition that subclause (b) takes account of our submission on Proposal 58-4.

> **Proposal 58–12** The Privacy Commissioner should address the following matters in the rules to be issued under the research exceptions to the proposed 'Collection' principle and the proposed 'Use and Disclosure' principle:
>
> (a) the process by which a Human Research Ethics Committee should review a proposal to examine a health information database or register to identify potential participants in research; and
>
> (b) the matters a Human Research Ethics Committee should take into account in considering whether the public interest in allowing the examination of the health information database or register outweighs the public interest in maintaining the level of privacy protection provided by the proposed UPPs.

Submission: APF supports Proposal 58-12, on condition that subclause (b) takes account of our submission on Proposal 58-4.

> **Proposal 58–13** Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should consult the Office of the Privacy Commissioner

to ensure that the systems or infrastructure they are developing meet the requirements of the Privacy Act.

Submission: APF supports Proposal 58-13 in principle. Though, as mentioned at Proposal 58-4, APF only supports the extension of research to non-health projects in the event that stronger privacy standards are retained. This is particularly important in relation to data linkage projects where non-health projects may seek to link non-health data to health data. Any consultations around this issue must therefore be conducted on the basis that there will be no weakening of relevant privacy standards.

DP72 Part I – Children, Yong People and Adults requiring assistance

Chapter 59. Children, Young People and Privacy

The APF welcomes the discussion on children's privacy in the ALRC Report. Such in-depth consideration of these issues is long overdue.

> **Proposal 59-1** The Australian Government should fund a longitudinal study of the attitudes of Australians, including young Australians, to privacy.
>
> **Proposal 59-2** The Office of the Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people.
>
> **Proposal 59-3** NetAlert should include specific guidance on using social networking sites as part of its educational material on internet safety.
>
> **Proposal 59-4** In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, and in particular privacy in the online environment, into school curricula.

Submission: The APF strongly supports Proposals 59-1, 59-2, 59-3 and 59-4 as important steps in overcoming the lack of attention to these matters in Australia to date.

Chapter 60. Decision Making by Individuals Under the Age of 18

At present the Privacy Act makes no distinction between adults and children – it applies equally to all. Nor does the Act contain any guidelines on how a decision maker might determine the capacity of someone to given informed consent on privacy matters. The ALRC Report aims to address this issue.

In its submission on the ALRC's Issues Paper 31, APF noted that there was no pressing reason to distinguish between adults and children in the Act, though there may be circumstances where this would be helpful. APF supported the development of further guidelines in this area to support the legislation. APF also emphasised the need to support children and young people in making decisions about privacy and to involve children wherever possible in decisions made regarding the handling of personal information about them, even where they were deemed not to have the capacity to do this in their own right.

> **Proposal 60–1** The *Privacy Act* should be amended to provide that:
> (a) an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable (in accordance with the criteria set out in Proposal 60–2) of giving that consent, making that request or exercising that right;
> (b) where it is practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, an assessment about the individual's capacity should be undertaken; and
> (c) where it is not practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, then the consent, request or exercising of the right to access must be provided by an authorised representative of the individual.
>
> **Proposal 60–2** The *Privacy Act* should be amended to provide that an individual aged under 18 is incapable of giving consent, making a request or exercising a right if, despite the provision of reasonable assistance by another person, he or she is incapable, by reason of maturity, injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability or any other circumstance, of:
>
> (a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

(b) communicating such consent or refusal of consent, making the request or personally exercising the right of access.

Where an individual under the age of 18 is considered incapable of giving consent, making a request or exercising a right, then an authorised representative of that individual may give the consent, make the request or exercise the right on behalf of that individual.

Proposal 60–3 The Office of the Privacy Commissioner should develop and publish guidance for applying the provisions relating to individuals under the age of 18, including on:

(a) the involvement of children, young people and their authorized representatives in decision-making processes;
(b) situations where children and young people are capable of giving consent, making a request or exercising a right on their own behalf;
(c) practices and criteria to be used in determining whether a child or young person is incapable of giving consent, making a request or exercising a right on his or her own behalf;
(d) the provision of reasonable assistance to children and young people to understand and communicate decisions; and
(e) the requirements to obtain consent from an authorised representative of a child or young person in appropriate circumstances.

The ALRC Report recommends in these proposals that, where possible, children and young people be assessed individually for capacity to provide consent about privacy matters. However, in acknowledgement of the fact that this may not always be practical, the ALRC also recommends that when a child cannot be individually assessed, children below the age of 15 be considered incapable of making decisions under the Act. (The age of 15 has been determined based on a range of factors discussed in the Report. It is also the age at which a person is currently entitled to access a Medicare Card without parental permission.) APF also understands that, in general, the option to individually assess children and young people would be the default option, with the proposed age of 15 being a fall-back option only.

In those circumstances where a specific age at which capacity is to be determined may be required, the APF supports the ALRC's recommendation of 15 years of age. This age reflects an appropriate balance between the, in general, autonomous capacity of 15+ year olds and at the same time providing appropriate protection for younger children.

Submission: The APF supports Proposals 60-1, 60-2 and 60-3 with the following provisos:

- To support this change, education for children and young people would be required on what their rights are under the privacy legislation (along the lines of the proposals outlined in Chapter 59).
- Priority should be given to assessing individual capacity on a case-by-case basis, and guidelines are needed to ensure that organisations and agencies do not take advantage of the proposed 15 age limit as a reason not to assess individually the capacity to consent where practical.
- Where an authorised representative is required (either because a person is under 15 or because they have been assessed as not having the capacity to make decisions about privacy on their own behalf), efforts still need to be made to involve the child or young person in the decision making process to the extent that this is practical.

The ALRC Report also discusses the liability of agencies and organisations in determining whether or not a person is under 15 years of age:

> **Proposal 60–4** The *Privacy Act* should be amended to provide that an agency or organisation will not be considered to have acted without consent if it did not know, and could not reasonably be expected to have known from the information available, that an individual was aged 14 or under, and the agency or organisation acted upon the consent given by the individual.

The APF acknowledges that it is sometimes difficult for an agency or organisation to tell whether or not they are dealing with someone under the age of 15. However, it is not clear from the proposal above exactly what might constitute an agency or organisation not knowing or not 'reasonably be(ing) expected to have known' about the age or capacity to consent of the person whose information they are dealing with. While APF acknowledges that the organisation or agency should not have to bear full liability in such situations, there is concern that the wording of this proposal places no obligation on the agency or

organisation to take steps to determine whether the consent assumed is adequate or not. At the least, an agency or organisation should be required to take 'reasonable steps' (perhaps 'where practicable') to determine if the consent given by an individual is informed or if consent from an 'authorised representative' is required. (This would be consistent with the slightly stronger approach reflected in the ALRC Proposal 61-3 below relating to adults with a temporary or permanent incapacity.)

AFP notes the ALRC's view that "this proposal (ie 60-4) should not be interpreted as allowing agencies and organisations to plead ignorance in every case due to a failure to establish appropriate age verification mechanisms" (para 60.108).

Submission: The APF strongly urges the ALRC to ensure that the onus for taking some responsibility for determining age and/or capacity to consent still remains with the agency or organisation handling the information.

The APF is particularly concerned that this approach be applied equally in online environments as it is not uncommon for children under the age of 15 to provide information online (as ALRC research confirms elsewhere in this Report).

> **Proposal 60–5** An agency or organisation that handles the personal information of individuals under the age of 18 should address in its Privacy Policy how such information is managed.
>
> **Proposal 60–6** An agency or organisation that regularly handles the personal information of individuals under the age of 18 should ensure that its staff are adequately trained to assess the decision-making capacity of children and young people.

Submission: APF supports proposals 60-5 and 60-6.

> **Proposal 60–7** Schools should clarify in their Privacy Policies how the personal information of students will be handled, including when personal information:
>
> (a) will be disclosed to, or withheld from, persons with parental responsibility; and
>
> (b) collected by school counsellors will be disclosed to the school management, persons with parental responsibility, or others.

Submission: APF supports proposal 60-7.

It is also noted that Proposals 60-1, 60-2 and 60-3 are relevant to the implementation of Proposal 60-7 in terms of ensuring that priority is given to undertaking an individual assessment of a young person's capacity to consent in relation to privacy matters. This is particularly important in relation to school counselling records, as noted earlier in the ALRC Report at paragraph 59.36. It is the view of the APF that it is unlikely that there would be any circumstances when the age of 15 and above for determining consent capacity would routinely apply in relation to use or disclosure of counselling records. Rather, a case-by-case assessment would be more appropriate.

> **Proposal 60–8** The Office of the Privacy Commissioner should include consideration of the privacy of children and young people in the proposed criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.

Submission: APF supports Proposal 60-8

Chapter 61. Adults with a Temporary or Permanent Incapacity

The APF acknowledges the complexities of the issues dealt with in this section, and welcomes the comprehensive coverage given to these matters in the Report.

> **Question 61–1** Should the *Privacy Act* be amended to provide expressly that all individuals aged 18 and over are presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable of giving that consent, making that request or exercising that right?

Submission: The APF supports the amendment suggested in Question 61-1.

> **Proposal 61–1** The *Privacy Act* should be amended to provide that an individual aged 18 or over is incapable of giving consent, making a request or exercising a right under the Act if, despite the provision of reasonable assistance by another person, he or she is incapable by reason of injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability, or any other circumstance, of:
>
> (a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or
>
> (b) communicating such consent or refusal of consent, making the request or personally exercising the right of access.
>
> Where an individual is considered incapable of giving consent, making a request or exercising a right under the Act, then an authorised representative of that individual may give the consent, make the request or exercise the right on behalf of the individual.
>
> **Proposal 61–2** The *Privacy Act* should be amended to introduce the concept of 'authorised representative', defined as a person who is, in relation to an individual:
>
> (a) a guardian of the individual appointed under law;
>
> (b) a guardian for the individual under an appointment of enduring guardianship;
>
> (c) an attorney for the individual under an enduring power of attorney;
>
> (d) person who has parental responsibility for the individual if the individual is under the age of 18; or
>
> (e) otherwise empowered under law to perform any functions or duties as agent or in the best interests of the individual.
>
> The *Privacy Act* should state that an authorised representative is not to act on behalf of the individual in any way that is inconsistent with an order made by a court or tribunal, in contravention of the terms of any appointment under law, or beyond the powers provided for in an enduring power of attorney.

Submission: The APF strongly supports Proposals 61-1. However in relation to Proposal 61-2, we support the submission by PIAC that the definition is too narrow and does not provide for more informal arrangements.

> **Question 61–2** Should the definition of 'authorised representative' include a person who was nominated by the individual at a time when the individual had the capacity to make the nomination?

Submission: In response to Question 61-2, the APF would support the inclusion of such arrangements in the definition of 'authorised representative'. Though, in addition to the mechanisms required to establish such a nomination, other mechanisms would be needed to ensure that the nomination remains up-to-date and is reviewed at such times in the future that the individual also has capacity to make such a nomination.

> **Proposal 61–3** The *Privacy Act* should be amended to provide that an agency or organisation that has taken reasonable steps to validate the authority of an authorised representative will not be considered to have engaged in conduct constituting an interference with privacy of an individual merely because it acted upon the consent, request or exercise of a right by that authorised representative, if it is later found that the authorised representative:
>
> (a) was not properly appointed; or

(b) exceeded the authority of his or her appointment.

Proposal 61–4 The Office of the Privacy Commissioner should develop and publish guidance for applying the provisions relating to individuals aged 18 and over incapable of giving consent, making a request or exercising a right on their own behalf, including on:

(a) the provision of reasonable assistance to individuals to understand and communicate decisions; and

(b) practices and criteria to be used in determining whether an individual is incapable of giving consent, making a request or exercising a right on his or her own behalf.

Proposal 61–5 Agencies and organisations that handle personal information about people incapable of making a decision should address in their Privacy Policies how such information is managed.

Proposal 61–6 Agencies and organisations that regularly handle personal information about adults incapable of making a decision should ensure that their staff are trained adequately to assess the decision-making capacity of individuals.

Submission: APF supports Proposals 61-3, 61-4, 61-5 and 61-6:

Chapter 62. Other third party arrangements

Proposal 62–1 Practice and procedures allowing for the involvement of third parties to assist an individual to make and communicate privacy decisions should be developed and published in guidance issued by the Office of the Privacy Commissioner.

Submission: APF supports the development of procedures to facilitate the involvement of third parties as outlined in Proposal 62-1.

Question 62–1 Should the *Privacy Act* be amended expressly to allow a third party nominated by the individual to give consent, make a request or exercise a right of access on behalf of the individual, either for one-off or long term arrangements?

The *Privacy Act* does not prevent the recognition of nominated third parties. Express recognition in the Act of nominated third parties, however, would provide further impetus and confidence for agencies and organisations to implement appropriate third party arrangements that involve decision making" (paragraph 62.19).

Submission: APF would only support such an amendment if it was supported by clear and tightly defined guidelines on how and when such an arrangement could be relied on. As the ALRC already notes, the Act has sufficient flexibility to ensure that third parties nominated by an individual can disclose and receive certain information with the consent of the individual. One of the unintended results of such an amendment could be a weakening of individual participation when it comes to decision making about personal information, hence the need for it to only apply in clearly defined circumstances. A mechanism to ensure that individuals are informed of any changes made under such arrangements would also ensure they are not open to abuse.

DP72 Part J – Telecommunications

[To follow]

End