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

Review of Privacy

Answers to questions in ALRC Issues Paper 31

http://www.alrc.gov.au/inquiries/current/privacy/index.htm

Australian Privacy Foundation submission to the Australian Law Reform Commission

January 2007

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

The APF welcomes the Inquiry and compliments the ALRC on a comprehensive and well presented Issues Paper. This submission follows the sequence of questions posed in the Issues Paper, chapter by chapter, and submits our view in response to each question, where we have formed one. The scope and breadth of the Paper, set alongside our reliance on volunteer membership, means that we have not be able to consider and respond to all the questions. Absence of a response does not indicate indifference or that we necessarily accept that the current regulatory position is satisfactory – only that we have not been able to offer a view in the timescale available.

The APF acknowledges the contribution made to this submission by the Interpreting Privacy Principles Project at the Cyberspace Law & Policy Centre at the University of New South Wales[1], whose detailed draft submission was made available to the APF.

1. Introduction to the Inquiry

1–1 Should the *Privacy Act* be amended to provide direct protection to groups such as: (a) Indigenous or other ethnic groups; or (b) commercial entities? If so, which groups or commercial entities should be covered by the Act?

No to (a). The right to privacy is inextricably linked to individual autonomy and dignity. To distinguish between different ethnic groups indicates that some individuals are deserving of more or less autonomy and dignity than others by virtue of their ethnic background. This is unacceptable, just as it would be unacceptable to temper our rights to freedom of speech and association on the basis of ethnicity. The example given in the issues paper, where Northern Territory privacy legislation protects against public disclosure of information about an

[1] see http://www.cyberlawcentre.org/ipp/

Aboriginal sacred site or tradition, appears to be a sensible means of keeping culturally sensitive information secure. It is not the basis of a separate standard of privacy protection for individual members of Indigenous or other ethnic groups. If particular 'problems' are encountered by specific groups, then they are likely to experienced more generally, and should be addressed generically.

No to (b) for three reasons. First, the right to privacy is a human right. How it is exercised varies from one individual to another, and from one social setting to another, but it is not transferable to government or commercial entities, or to any other institution or group created by groups of individuals within the community. Such organisations can be transformed or dismantled at any time and their activities and powers wax and wane. They have no inherent rights of their own. Second, the trend in law reform concerning corporations and other commercial entities is for greater accountability and transparency to their shareholders, customers, employees and the wider community. Commercial entities are now required by law to disclose a great deal of information, and these requirements would override any privacy rights that could be created for them. Third, commercially sensitive information is already protected by various laws such as intellectual property laws, the general law duties of fidelity and confidentiality and the use of restrictive convenants in employment contracts. Giving corporate entities privacy rights opens up prospect of their use for commercial disputes, potentially damaging the image and credibility of privacy laws, which should remain true to their human rights origins and focus on protecting individuals

1–2 Should a cause of action for breach of privacy be recognised by the courts or the legislature in Australia? If so, and if legislation is preferred, what should be the recognised elements of the cause of action, and the defences? Where should the cause of action be located? For example, should the cause of action be located in state and territory legislation or federal legislation? If it should be located in federal legislation, should it be in the *Privacy Act* or elsewhere?

A specific cause of civil action – a statutory privacy tort – would be a useful complement to privacy laws. We reserve our position on the detail of such an innovation, which we understand the NSW LRC will be consulting on specifically.

Additional submission

We acknowledge that the ALRC has chosen to focus primarily on information privacy, and to a lesser extent on communications privacy (paragraph 1.89). However, we note that the terms of reference are not so restricted and submit that the ALRC should either separately review wider aspects of privacy such as bodily and territorial privacy and surveillance, or recommend to the government that this wider review be conducted as a subsequent exercise. Such a review should address the desirability of a general presumption in Australian law against unreasonable search and seizure, as embodied in the Fourth Amendment to the US Constitution. This could be provided through a statutory Bill of Rights.

2. Overview of Privacy Regulation in Australia

2–1 Is national consistency in the regulation of personal information important? If so, what are the most effective methods of achieving nationally consistent and comprehensive laws for the regulation of personal information in Australia?

Consistency is a valuable objective, but should not be pursued to the detriment of the level of protection. Levelling up is good, but levelling down is undesirable. It would not be desirable to have a referral of powers, leaving only a federal law – having several privacy regulators is a healthy way of ensuring peer review and promoting high standards in performance of their functions. It would ensure that citizens in each jurisdiction have a regulator they can go to for advice and to handle complaints and which can undertake local community education programs. Similarly, organisations that are subject to local privacy laws have access to a local regulator

who is aware of their circumstances and can provide advice and training on implementing the legislation.

The federal, State and Territory governments should each be directly responsible and accountable for the decisions they make concerning the information they collect from the public. Separate privacy laws for the public sector in each jurisdiction should be maintained or established, covering all publicly funded entities and publicly funded projects. This could best be achieved by mirror legislation or a complementary law regime. We would support interim provisions in a federal law that could apply to the jurisdictions that do not yet have a privacy law and which could be 'rolled back' upon the introduction of a local equivalent law.

At the same time, we can see benefit in having a federal law for the private sector, for which state borders are often irrelevant, or should be irrelevant, to their operations. The issue for consistency in this sense is for coverage across the entire private sector, and not the current piecemeal approach.

We do not support the establishment of a permanent, overarching, standing body on privacy. Such bodies have delayed or buried privacy issues in the past. The Issues Paper mentions the Health Privacy Working Group of the Australian Health Ministers' Advisory Council, which is a poor example. It has failed after many years to produce a national health privacy code, the most recent public draft of which was released in 2003. The Standing Committee of Attorneys General has similarly been unsuccessful in tacking national privacy issues.

3. The *Privacy Act 1988* (Cth)

3–1 Is the structure of the *Privacy Act* logical? Does the *Privacy Act* need to be redrafted to achieve a greater degree of simplicity and clarity?

It should be possible to simplify the Act – some of the definitions and their interaction with the application provisions and exemptions are particularly 'opaque'. Only one set of principles should apply to both private and public sectors, but there is no reason why there should not be specific sectoral rules (as now for credit reporting and TFNs) where these can be justified.

3–2 Insofar as the *Privacy Act* is primarily concerned with data protection, is the name of the *Privacy Act* accurate and appropriate?

Information Privacy Act (as in Victoria) would be a better name. 'Data protection', though used in Europe and elsewhere, is not familiar to the public in Australia and runs the risk of misleading – the law is not and should not be just about computerised information, and 'data protection' also re-inforces the unfortunate perception that it is just about security.

3–3 Is there some benefit in amending the *Privacy Act* to include the objects of the legislation? If so, what should be included in the objects clause?

This could both assist courts and tribunals in interpreting the law, and also assist in promoting public and data user awareness of the law. However, we would be opposed to an objects clause similar to that in the Privacy Amendment (Private Sector) Act 2000 that promoted 'the free flow of information' to a right to be balanced against privacy rights. An Information Privacy Act must remain primarily about the protection of a fundamental human right. The objects should be along the lines of the ' purposes' of the Victorian Information Privacy Act (s.1).

3–4 Are the definitions in the *Privacy Act* adequate and appropriate? For example, are the definitions of 'personal information' and 'sensitive information' in the *Privacy Act* adequate and appropriate?

Personal information needs to be defined as any information from which an individual can be identified, whether from the information itself or by reference to other information in the possession of, or readily accessible to, the data user. This would ensure that information such as telephone numbers, email or IP addresses, and information stored with an identifier code or label rather than a name, are covered .

Sensitivity is contextual, and it trying to define sensitive information in advance runs the risk of placing unnecessary constraints on data users for whom particular information is mundane and uncontroversial, such as religion for churches, health information for hospitals and trade union membership for trade unions. The same information in the hands of other data users can indeed be highly sensitive. The current definition of sensitive information in the Act does not include financial information, which many individuals find surprising..If sensitive information is to be defined and made subject to additional rules, it makes no sense for that to only be the case for the private sector, as now.

3–5 Should the definition of 'personal information' in the *Privacy Act* be amended to include personal information of the deceased?

The APF does not have a strong view on this issue – there are good arguments both for and against extending privacy rights to a period after death. The protection of information about deceased people is primarily a matter of confidentiality and the implications for the living of how the information is used and disclosed. Not all the principles can sensibly apply, since the person cannot be notified or consulted about how their information is handled. It may be preferable to write specific provisions that directly address this issue than to simply extend the definition of personal information.

4. Examination of the Privacy Principles

4–1 Are the obligations imposed on **organisations** at the time of collection of personal information adequate and appropriate? For example, should an organisation also be required to make an individual aware of (a) the types of people, bodies or agencies to whom the organisation usually discloses information of that kind; (b) the various avenues of complaint available; and (c) the source of the information, where it has not been collected directly from the individual?

The principle should require all organisations to identify the party or parties to the transaction, and to expressly require operative contact details to be given.

While the principle can expressly allow generic descriptors of disclosure (as NPP 1.3(d) does now) it should also include an obligation to answer specific enquiries about whether a particular named agency or organisation is a recipient (this may be better included in the openness principle – we suggest later that the notification and openness principles be rationalized).

The principle should require organisations to notify individuals of both internal and external dispute resolution options

We are sympathetic in principle to the concept of layered privacy notices, the Discussion Paper should canvass views about the minimum set of information which needs to provided at or before the time of collection to achieve the objective of the awareness principle, and the minimum standard of transparency of links to more detailed information.

4–2 Should NPP 1 be amended to clarify that there may be circumstances in which it is reasonable for organisations to take no steps to ensure that an individual is aware of specified matters relating to the collection of personal information?

This is unnecessary. Guidance material can explain that this is a possibility, together with examples. The addition of wording such as 'if any' would invite self serving interpretation to avoid giving notice even where it was both reasonable and practicable.

4–3 Are the obligations imposed on **agencies** at the time of collection of personal information adequate and appropriate? In particular, should agencies also be subject to a general requirement that where reasonable and practicable, they should collect information about an individual only from the individual concerned? Should agencies also be required to notify an individual of his or her rights of access to the information, the consequences of not providing the information, the various avenues of complaint available, and the source of the information, where it has not been collected directly from the individual?

There is no good reason why Commonwealth agencies should not have the same obligation as NSW, Victorian and NT government agencies, and private sector organisations, to collect wherever possible directly from the data subject.

The wording of a 'direct collection' principle should be based on NPP 1.4 but should omit 'only' which appears redundant and does not readily accommodate situations where some information can be obtained directly with supplementary information justifiably obtained from a third party.

Agencies should be subject to the same notification requirements as private sector organisations.

The law should make it clear that the collection principles apply to the maximum practical extent to information obtained from observation or surveillance. It may be appropriate for there to be some relaxation of the notice requirements, but this should be integrated with the specific requirements of surveillance laws.

The law should make it clear that the collection principles apply to the maximum practical extent to information extracted from other records. There will be some circumstances where it is undesirable and unnecessary to impose notice requirements for collection from documentary sources, especially where personal information is incidental to the purpose of the data user (e.g. authors, historians, researchers)

4–4 Should any obligations attach to an agency or organisation which receives unsolicited personal information that it intends to include in a record or generally available publication? If so, what obligations should be imposed?

The law should make it clear that collection principles apply, to the maximum practicable extent, to unsolicited information.

4–5 Should the obligations imposed on an organisation or agency at or soon after collection apply irrespective of the source of personal information?

All collection obligations should apply to the extent practicable irrespective of the source, subject to the qualifications in our answers to Q 4-3. There is no need to exhaustively address all of the possible sources and practicalities – expressing the principle in this way would allow for reasonable exceptions, to be justified on a case by case basis by data users when addressing compliance, and if challenged.

The law should make it clear that collection can only be lawful if the purpose is also lawful. Consideration should be given to Australian law adopting a 'purpose justification' test along Canadian, European or other appropriate lines.

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

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.

4–6 Is it desirable for the IPPs to deal separately with the principles relating to the use and disclosure of personal information or should use and disclosure be provided for in one principle?

The use principle should clarify whether accessing personal information, without further action being taken as a result of that access, is 'use' of personal information.

Privacy laws should make it clear that even information already known to the recipient can still be 'disclosed'.

4–7 Are the circumstances in which agencies and organisations are permitted to use and disclose personal information under IPPs 10 and 11, and NPP 2, adequate and appropriate? In particular, should agencies and organisations be permitted expressly to disclose personal information: (a) to assist in the investigation of missing persons; (b) where there is a reasonable belief that disclosure is necessary to prevent a serious and/or imminent threat to an individual's safety or welfare, or a serious threat to public health, public safety or public welfare; and (c) in times of emergency? What mechanism should be adopted to establish the existence of an emergency?

The law should be clarified to expressly allow for the declaration of multiple specific purposes, where collection is necessary for each of these purposes (but see our response to Q 4-11). The exception for mere awareness of disclosure practices without consent to them should be removed.

The ALRC should review the justification for the recent amendments concerning emergencies, which were given relatively little scrutiny in Parliament.

4–8 Are the criteria in NPP 2.1(a) for using personal sensitive and non-sensitive information for a secondary purpose adequate and appropriate? For example, is it necessary or desirable that there also be a 'direct' relationship between the secondary and primary purpose of collection before non-sensitive personal information can be used or disclosed for a secondary purpose?

The general adoption of 'directly related' in the related purposes test is appropriate.

4–9 Is the scope of IPP 10(e) (which allows agencies to use personal information for a purpose other than the particular purpose of collection, if the purpose for which the information is used is directly related to the purpose of collection) adequate and appropriate? For example, should there be an additional requirement that the individual concerned would reasonably expect an agency to use the information for that other purpose?

The 'reasonable expectations' test is desirable as part of a test of related purposes.

4–10 In what circumstances should agencies or organisations be required to record their use or disclosure of personal information when it is used or disclosed for a purpose other than the primary purpose?

There should be a general requirement to record uses and disclosures for secondary purposes. This need not involve annotating individual records where information is used or disclosed in bulk, but some record should be kept to allow reconstruction in the event of enquiry or challenge (see our submission in response to Q 4-1), to allow notification of third parties where information is subsequently corrected (Q 4-25) and to allow notification of individuals in the event of security breaches (see our endorsement of a new principle at Q 4-35)

4–11 Are there particular issues or concerns arising from the practice of organisations seeking bundled consent to a number of uses and disclosures of personal information? If so, how are these concerns best addressed?

The law should be clarified concerning 'bundled consent', in order to avoid abuse. It is particularly important that data users not be allowed to bundle genuine consent for optional uses along with so-called consents which are in reality mere acknowledgements of conditions.

4–12 Is it appropriate that NPP 2 allows for personal non-sensitive information to be used for the secondary purpose of direct marketing? If so, are the criteria that an organisation needs to satisfy in order to use personal information for direct marketing purposes adequate and appropriate?

NPP 2 does not deal adequately with direct marketing and this has led directly to the need for two separate laws – the Spam Act 2003 and the Do Not Call Register Act 2006. Neither of these laws would be necessary if there was a properly functioning use and disclosure principle in the Privacy Act, together with adequate sanctions and active enforcement. Both Acts effectively set up an 'opt-out' regime where marketers have to respect the clearly expressed preference of an individual not to receive unsolicited marketing. The same effect would be achieved if NPP 2 clearly identified unsolicited direct marketing as a secondary use which required express or implied consent.

Privacy law should contain a sub-principle dealing expressly with direct marketing, broadly defined, unequivocally giving individuals a right to opt-out of receipt of further communications from private sector organisations. Such a principle needs to be designed to be consistent with other more specific legislation, which may however continue to apply a higher standard in relation to particular types or modes of communication.

Consideration should be given to providing a right to opt-out of direct marketing from government agencies – subject perhaps to limited exemptions for public health and safety campaigns or where government agencies had specific knowledge of individuals eligibility.

Privacy law should require that data users take reasonable steps, on request, to advise an individual from where they acquired the individual's personal information.

4–13 Should use and disclosure of personal information be allowed for research that does not involve health information—for example social science research? If so, in what circumstances or upon what conditions might this be appropriate?

This depends on the definition of research – see our response to Q 8-26.

Additional submission

The disclosure principle should include an obligation on any recipient of personal information to only use (or further disclose) the information for the purposes for which it is provided or where expressly required by law. This would avoid an 'endless' chain of function creep where each recipient can take advantage of any of the non-disclosure exceptions. A precedent exists for this additional obligation in Part 13 of the Telecommunications Act 1997 (s.297)

4–14 Is the scope of the data quality principle in NPP 3 (which requires an organisation to take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date) adequate and appropriate? For example, should the principle expressly apply to information that an organisation controls?

The data quality principle should define quality as including the qualities of accuracy, completeness, relevance and currency. It should apply to information that an organisation controls.

4–15 Is there a need to amend NPP 3 to clarify the extent of the obligations of an organisation under the data quality principle or is this best dealt with by way of guidance issued by the Office of the Privacy Commissioner?

This should be dealt with by guidance.

4–16 Should agencies be subject to a stand-alone data quality principle that extends to the collection, use and disclosure of personal information?

The law should apply a 'reasonable steps' data quality principle to all data users both at the time of collection and prior to use.

4–17 Is the scope of NPP 4 relating to the obligations of an organisation to secure data adequate and appropriate? For example, should NPP 4 be amended to impose an obligation on organisations to take reasonable steps to ensure that personal information they disclose to contractors is protected?

Based on a comparative analysis of various privacy instruments, the draft Asia Pacific Privacy Charter proposed the following model security principle:

> *"Organisations should protect personal information against unauthorised or accidental access, use, modification, loss or disclosure, or other misuse, by security safeguards commensurate with its sensitivity, and adequate to ensure compliance with these Principles".*

The Security Principle in the more recent APEC Privacy Framework is arguably even more comprehensive:

> *"Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment."*

We submit that a security principle constructed from these two models should apply to all data users.

4–18 Are there any circumstances in which agencies should be under an obligation to destroy or permanently de-identify personal information when it is no longer needed?

Privacy law should address retention and disposal in an independent principle applying to all data users.

4–19 Should the IPPs and the NPPs regulate the deletion of personal information by organisations and agencies? In what circumstances might this be appropriate? Should an individual have the right to request that an agency or organisation destroy personal information that it holds or controls concerning the individual? If so, in what circumstances or upon what conditions should this be permitted?

A retention and disposal principle should require data users to destroy or permanently de-identify personal information when it is no longer needed either for the purpose of collection or for any other purpose for which it has legitimately already been used, or as required by law. Secondary purposes for which personal information could <u>prospectively</u> be used or disclosed should not provide an alternative justification for retention.

4–20 Is the scope of NPP 5 relating to openness adequate and appropriate? For example, is it necessary or desirable for organisations to be given greater legislative guidance about their obligations under the principle? Does the more prescriptive approach to the openness principle in IPP 5 provide a suitable model?

The Discussion Paper should canvass the possibility of a combined 'awareness' principle, covering both notification requirements at the time of collection and more general information provision, and with specific attention to the respective roles of proactive notice vs obligations to respond to enquiries.

The Digest provisions should remain. Even if the compilation and publication of a central Digest were to be discontinued, the obligation on agencies to maintain individual records and make these available for public inspection (IPP 5.4(a)) should remain.

Privacy law should give the Commissioner the discretion to require organisations to publish further information about particular personal information handling projects.

4–21 Is it appropriate that certain obligations under the NPPs relating to openness are triggered only upon an individual's request?

Yes – see our response to Q 4-1.

4–22 Is there a need to clarify the relationship between the obligation of an organisation under NPP 1.3 (which imposes an obligation on organisations to take reasonable steps to ensure that an individual is aware of specified matters at or before the time of collection) and NPP 5.1 (which imposes an obligation on organisations to set out in a document clearly expressed policies on its management of personal information)? If so, how is this best achieved?

Yes – see our support in response to Q 4-20 for a combined awareness principle

4–23 Are the circumstances in which organisations can deny an individual access to his or her personal information under NPP 6 adequate and appropriate? If the circumstances are inadequate, should this be addressed by legislative amendment to the principle or by guidance issued by the Office of the Privacy Commissioner?

This needs to be answered in the context of a rationalisation of the Privacy and FOI Acts. We reserve our position but generally support the ALRC's 1995 recommendations in Report 77.

4–24 Should IPP 6 more clearly set out the circumstances in which agencies can deny an individual access to his or her personal information? If so, what circumstances should be included?

This needs to be answered in the context of a rationalisation of the Privacy and FOI Acts. We reserve our position but generally support the ALRC's 1995 recommendations in Report 77.

4–25 Should the *Privacy Act* be amended to impose an obligation on both agencies and organisations to notify third parties, where practicable, that they have received inaccurate information and to pass on any corrected information? Should an obligation to notify third parties apply where agencies or organisations have refused to make a correction?

The law should require data users to notify third parties, where practicable and at the express request of the individual concerned, that they have received inaccurate information and to pass on any corrected information.

Additional submissions in relation to correction

Correction obligations should apply independently of rights of access – i.e. the right of individuals to seek correction should apply whether they have obtained access through formal processes (such as under the Privacy or FOI Acts) or have become aware of the information by other means.

The principle should make it clear that correction can take the form of amendment, deletion or addition, as appropriate in the circumstances. There are many situations where there is a legal

requirement to keep a historical record of actual transactions, but this should not prevent the correction of 'operational' records, leaving the original incorrect information only in an archive.

The principle 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.

4–26 Is there a need for a separate privacy principle regulating the adoption, collection, use and disclosure of identifiers by organisations? Should NPP 7, the principle regulating identifiers, be redrafted to deal more generally with the issue of data-matching?

In relation to identifiers – see our response to Chapter 12 and Q 7(g). In relation to data-matching, see our response to Q 7(h).

4–27 Is the definition of identifier adequate and appropriate? Are the exceptions to the use and disclosure of identifiers referred to in NPP 7 adequate and appropriate? Should an individual be permitted to consent to the use of his or her unique identifier? If so, in what circumstances and by what means should this exception be given effect?

See our responses to Chapter 12 and Q 7(g)

4–28 Should the *Privacy Act* be amended to regulate the assignment, adoption, collection, use and disclosure of identifiers by agencies?

See our responses to Chapter 12 and Q 7(g)

4–29 Should NPP 8, the anonymity principle, be redrafted to impose expressly an obligation on organisations to give an individual the option of remaining anonymous when entering into transactions with those organisations?

The anonymity principle should be retained but redrafted to include the concept of pseudonymity as an alternative where appropriate. The principle should also clarify that it 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.

The anonymity principle should impose an obligation on organisations to give an individual the option of remaining anonymous or pseudonymous (as appropriate) when entering into transactions. The touchstone remains 'minimum collection necessary for the purpose of the transaction'.

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

4–30 Is it appropriate or desirable for agencies to be subject to an anonymity principle? In what circumstances, if any, might this be appropriate?

The anonymity/pseudonymity principle should also apply to the public sector.

4–31 Should the transfer of personal information offshore by agencies be regulated by privacy principles?

The transfer of personal information across any jurisdictional boundary, not just offshore, by any data users should be regulated – see our response to Chapter 13.

4–32 Should federal privacy principles allow agencies and organisations to collect non-health related sensitive information for other purposes, including research and statistical purposes? If so, in what circumstances should this be permitted?

See our response to Q 8-26

4–33 Should federal privacy principles establish a separate regime for the public and private sectors regulating sensitive information in all aspects of the information cycle, including collection, use, disclosure, storage, access, retention and disposal? If so, what should that regime include?

See our response to Q 3-4. If sensitive information remains separately defined, then any additional requirements relating to this information should apply to all data users. If it is considered appropriate to retain the additional collection principles for sensitive information, then there should also be additional use and disclosure principles to similar effect. Data users will often be able to justify the collection of sensitive information on the basis of their primary purpose, but any secondary uses should be subject to a separate test on the same criteria as collection.

4–34 Should the *Privacy Act* provide a uniform set of privacy principles that are to apply to both the public (currently covered by the IPPs) and private (currently covered by the NPPs) sectors? If so, what model should be used? Are there any particular principles or exceptions to principles that should apply only to either the public or private sector?

There should be a single set of principles to apply to both Commonwealth agencies and private sector businesses (and ideally to all State and Territory public sector agencies and to all other organisations including those currently exempt from any of the existing laws). We submit that there are no particular principles that should apply only to either the public or private sector, but that there are exceptions which will be more or less relevant to different sectors. There is no single existing model which should be preferred as all have been shown to have weaknesses – a new set of common principles should be derived from analysis of the various precedents. In some cases the resulting principles will be very close to the existing NPPs or IPPs, thereby minimising any adjustment of compliance requirements.

4–35 Apart from the principles contained in the IPPs and NPPs, are there any other principles to which agencies and organisations should be subject? For example, should the IPPs and NPPs include expressly: an 'accountability' principle; a 'prevention of harm' principle; a 'consent' principle; or a requirement that agencies and organisations notify persons whose personal information has been, or is reasonably believed to have been, accessed without authorisation? If so, what should be the content of these principles?

Privacy laws should provide for organizations or groups of organizations to voluntarily adopt governance rules or standards relating to personal information which could then be made binding by registration with the Privacy Commissioner. This would allow organisations to gain consumer trust by committing to measures such as privacy impact assessments (see below and our response to Q 6-6) and audits (see our response to Q 6-10)

Privacy law should include an additional no-disadvantage principle to ensure that data users do not use pricing or other sanctions to deter individuals from exercising their privacy rights.

Privacy law should require data users to notify individuals affected by a breach of security. We agree with the ALRC (paragraph 4.206) that the threshold criteria for triggering a notification requirement is critical. There should by now be enough experience of the US State Security Breach Notification laws to guide a sensible rule.

Privacy law should require Privacy Impact Assessments for significant projects (see also Q 6-6)

Consideration be given to an automated decision-making principle which requires human intervention before any adverse action is taken in relation to any individual based solely on automated processes.

.

4–36 Should federal privacy principles be prescriptive or should they provide high-level guidance only? Should they aim for a minimum or maximum level of protection of personal information or aim to adopt a best practice approach?

We submit that it is desirable to adopt principles (i) which are consistent, at least within Australia, and (ii) which represent best practice in terms of promoting internationally accepted privacy standards.

5. Exemptions from the *Privacy Act 1988* (Cth)

5–1 Is it appropriate for certain entities to be exempt, either completely or partially, from the operation of the *Privacy Act*? If so, where should the exemptions be located?
There is no justification for any agency or organisation being wholly exempt from the Privacy Act, other than:

- *Individuals handling personal information solely for non-business purposes (s.7B(1)), (objectionable practices by individuals such as voyeuristic photography, internet publication of unwelcome information about another individual etc are best dealt with by other civil law measures, including a tort of privacy, and criminal laws where appropriate), and*

- *Organisations or agencies subject to another equivalent privacy law (see under Chapter 13 for discussion of criteria for equivalence) – see also Q 5-4.*

5–2 Should the following defence and intelligence agencies be exempt, either completely or partially, from the *Privacy Act*:

- Defence Imagery and Geospatial Organisation;
- Defence Intelligence Organisation;
- Defence Signals Directorate;
- Australian Security Intelligence Organisation;
- Australian Secret Intelligence Service; and
- Office of National Assessments?

If so, what is the policy justification for the exemption? Are there any other defence and intelligence agencies that should be exempt, either completely or partially, from the *Privacy Act*?

We accept that there may need to be specific exemptions from some privacy principles (principally the collection and access principles) for some intelligence agencies, but there is no justification for these agencies not to be subject to all of the principles in respect of administrative and employment information, or for them to be exempt from, for example, the security and quality principles, even for the personal information they collect operationally.

The fact that access, correction and review and complaint rights might need to be qualified for operational data does not justify lifting the obligation to keep information secure, maintain data quality and delete information once no longer required. The reasonable steps qualification to these principles should adequately deal with the special circumstances of these agencies.

Similarly there is no reason why the use and disclosure principles should not apply, with a specific exception similar to that provided in the context of access in NPP 6.1(k) in addition to the normal range of required by law and 'prejudice to law enforcement' exceptions – see below.

5–3 Should the following agencies be exempt, either completely or partially, from the *Privacy Act*:

- Australian Government ministers;
- federal courts;
- agencies specified in Schedule 1 to the *Freedom of Information Act 1982* (Cth)—namely, the Australian Industrial Relations Commission, the Australian Fair Pay Commission, the Industrial Registrar and Deputy Industrial Registrars;
- Australian Crime Commission;
- royal commissions;
- Integrity Commissioner;
- agencies specified in Schedule 2 Part I Division 1 of the *Freedom of Information Act 1982* (Cth) other than the intelligence agencies, the Australian Government Solicitor and the Australian Industry Development Corporation; and
- agencies specified in Schedule 2 Part II Division 1 of the *Freedom of Information Act 1982* (Cth)?

If so, what is the policy justification for the exemption? Are there any other agencies that should be exempt, either completely or partially, from the *Privacy Act*?

As for intelligence agencies, there is no justification for wholesale exemption. Any difficulties that compliance with privacy principles might cause for any of these agencies should be dealt with by means of selective exceptions to particular principles and provisions, but only on the basis of detailed justification. If the concern is about one 'watchdog' having oversight of another, we reject any suggestion that this a bad thing – no agency, however important the public policy purpose it is performing, should be exempt from the obligation to comply with fundamental human rights and administrative law principles.

5–4 Should state and territory authorities be exempt from the privacy principles in the *Privacy Act*?

Yes to the extent that they are subject to equivalent privacy laws (see discussion of equivalence criteria under Chapter 13). To the maximum extent constitutionally possible the federal law should cover public sector agencies in states without an equivalent law.

5–5 In addition to the energy distributors owned by the New South Wales Government, which are the only state authorities prescribed under the *Privacy (Private Sector) Regulations 2001* (Cth), are there any other state or territory authorities that should be covered by the privacy principles in the *Privacy Act*? If so, to what extent should they be covered?

The law should make provision for coverage of any state or territory authorities 'by agreement' (effected through Regulations) to cover the increasing number of 'hybrid' organisations involved in the delivery of public services and to ensure no organisation can 'fall between the gaps'.

5–6 Should the small business exemption remain? If so: (a) what should be its extent; and (b) should an opt-in procedure continue to be available?

The small business exemption threshold is completely arbitrary. It is impossible to envisage any sensible size or other criteria which would capture potentially significant personal information

handling while excluding 'mundane' processing. Even one-person businesses can be at the forefront of privacy intrusion (e.g. private investigators, or specialised websites).

The sensible response is to have a default position of all businesses being subject to the privacy principles, but with an overall reasonable steps qualification applying to all principles. This would allow the Privacy Commissioner to issue guidance about the circumstances in which no steps, or only limited steps, would be reasonable. For most small businesses, no pro-active steps would be required (even in relation to notice), and while a promotional campaign could encourage them to review their operations, some may only become aware of their obligations if and when they receive a complaint.

5–7 Should registered political parties be exempt from the operation of the privacy principles in the *Privacy Act?*

There is absolutely no justification for political parties to be exempt – most individuals, if they were aware of the increasingly sophisticated database operations of political parties, would see them as clear examples of personal information processing needing the protection of the privacy principles.

5–8 Should political acts and practices be exempt from the operation of the *Privacy Act*? If so, does the current exemption under s 7C of the *Privacy Act* strike an appropriate balance between the protection of personal information and the implied freedom of political communication?

There can be no justification for political acts and practices to be wholly exempt. If compliance with any of the principles causes difficulties that interfere with the legitimate and desirable operation of representative democracy, then a specific exception may be justified. To the extent that there is an implied constitutional right to freedom of political expression and communication this surely does not go as far as forcing information onto an individual who has expressed a clear preference not to receive it. There are many alternative means for politicians to make their pitch to electors without giving them a right to keep secret databases and make unsolicited direct approaches. No-one has ever attempted to justify why the basic principles of notification, data quality and security, and access and correction cannot apply to personal information used in political acts and practices – probably because it would be impossible to do so.

5–9 Should the employee records exemption remain? If so: (a) what should be the scope of the exemption; and (b) should it be located in the *Privacy Act*, workplace relations legislation or elsewhere?

There is no justification for the private sector employee records exemption, and it represents one of the major gaps and weaknesses in the Privacy Act. Experience in other jurisdictions (including the IPP regime applying to Commonwealth agencies) shows that employees are major users of privacy rights. This is unsurprising given that the implications of non-compliance can be very far-reaching and serious in an employment context. The federal government's assurances that privacy interests of employees are adequately addressed by employment law are worthless. The inter-departmental working group set up in 2001 to review the employee record exemption has yet to report, probably because it would have to conclude that there is no effective privacy protection for private sector employees.

5–10 Should acts and practices of media organisations in the course of journalism be exempt from the operation of the *Privacy Act*? If so: (a) what should be the scope of the exemption; and (b) does s 7B(4) of the *Privacy Act* strike an appropriate balance between the free flow of information to the public and the protection of personal information?

The exemption for media organisations is far too broad – journalism is not defined and the definition of media organisation effectively allows anyone to claim the exemption by setting up a 'publishing' enterprise. The condition requiring a public commitment to privacy standards can be satisfied by the organisation itself, with no independent assessment.

There are serious issues about the balance between privacy rights and freedom of expression, and about the legitimate public interest role of the media, but these issues should be addressed with selective exceptions to some of the principles, if justified, rather than by a blanket exemption.

5–11 Should the terms 'in the course of journalism', 'news', 'current affairs' and 'documentary' be defined in the *Privacy Act*? If so, how should they be defined? Are there other terms that would be more appropriate?

See our answer to Q 5-10 above. If there are to be selective exceptions for public interest media activity, these terms will need to be much more carefully and closely defined. While difficult, it must be possible to distinguish between genuine news and current affairs journalism which deserve some exemption, and the infotainment, entertainment and advertising which makes up the bulk of media content and which should be subject to privacy principles to the maximum extent practicable.

5–12 If the media exemption is retained, how should journalistic acts and practices be regulated?

See our answers to Qs 5-10 & 5-11 – we do not believe the media exemption should remain in its current form

5–13 Do any issues arise concerning related bodies corporate, changes in partnership and overseas acts required by foreign law in Part III Division 1 of the *Privacy Act*? If so, how should they be dealt with?

We are concerned that the related bodies corporate exemption in s.13B is too broad and results in uses of information being allowed which are contrary to the reasonable expectations of individuals. Many corporate relationships are obscure and customers of one trading enterprise are often unaware of other ownership or control relationships. The law should require businesses to legitimise transfers of information to related bodies corporate by informing individuals. There seems no reason to have a special exemption – businesses should be able to meet one of the tests in the exceptions to NPP2.

5–14 Are there any other entities or types of activities that should be exempt from the operation of the *Privacy Act*? If so, what are those entities or types of activities, and what should be the scope of the exemption?

We do not see the need for any total exemptions, and are not aware of any other entities or types of activities which need selective exceptions. Carefully designed selective exceptions should be able to accommodate any new or currently unrecognised compliance difficulties

6. Powers of the Office of the Privacy Commissioner

6–1 Is the legislative structure pertaining to the Office of the Privacy Commissioner established under the *Privacy Act* appropriately meeting the needs of the community?

It is clear that the Office of the Privacy Commissioner, while performing many valuable functions, is not currently meeting the legitimate expectations of the community, either in relation to complaint handling or in relation to wider roles of advocacy and pro-active enforcement. The Office is widely perceived as a 'paper tiger' whose advice and guidance, if available at all, is often far too accommodating of government and business practices which are contrary to either the letter or the spirit of the privacy principles. Even where the Office does form a view that a principle has been breached, only minor remedies and sanctions are imposed. Most data users, in government and business alike, understandably take a risk management approach to privacy compliance and any such assessment is likely to lead to privacy being given a low priority.

The extent to which this overall failing is due to the structure of the Act as opposed to the exercise of their functions by successive Commissioners is difficult to identify clearly. The powers and functions of the Commissioner appear on paper to be both comprehensive and strong, although there are some marginal changes that could usefully be made.

6–2 Are the constraints imposed in the *Privacy Act* on the exercise by the Privacy Commissioner of powers conferred by the Act appropriate?

Successive Privacy Commissioners appear to have interpreted s.29(a) of the Act as limiting their ability to perform the role of public advocate and champion of privacy. We submit that this is an unfortunate and unnecessary interpretation.

6–3 Does the Privacy Advisory Committee perform a useful role and have appropriate powers and functions? Are the fields of expertise represented on the Privacy Advisory Committee appropriate? Does the Privacy Advisory Committee, and the fields of expertise of Privacy Advisory Committee members, need to be set out in the *Privacy Act*?

The Privacy Advisory Committee may perform a useful function 'behind the scenes' but is almost invisible to the public. Members do not seem to have seen themselves as accountable to the constituencies which might be inferred from the criteria for appointment and have rarely sought to consult with constituencies.

The objectives of the Advisory Committee might be better performed by separate committees representing business, government and consumer interests respectively, with independent secretariats and public reporting requirements.

6–4 Is the scope of immunities conferred on: (a) the Privacy Commissioner and his or her delegates; (b) an adjudicator appointed under a privacy code and his or her delegates; and (c) other persons, appropriate?

It is important that the Privacy Commissioner and any other adjudicators appointed under the Act have immunity (currently under s.64) and that complainants and respondents also have protection from civil action for acts done in good faith (currently under s.67). The law should confirm that this protection extends to bodies bringing representative complaints and otherwise drawing privacy compliance issues to the attention of the Commissioner and the public

.

6–5 Are the Privacy Commissioner's powers to oversee the *Privacy Act* appropriate and exercised effectively? For example, are the Commissioner's powers: (a) to furnish advice; (b) to research and monitor developments in data processing and computer technology; (c) to promote understanding of the IPPs and of the objects of the IPPs and the NPPs; (d) to undertake education programs to promote individual privacy protection; (e) relating to tax file numbers; (f) arising under other Acts, appropriate and exercised effectively?

As already suggested in our answer to Q 6-4, we believe the Commissioner's powers are generally appropriate and adequate but are not exercised as effectively as they could be.

6–6 Should the *Privacy Act* require a privacy impact assessment to be prepared for: (a) all proposed Commonwealth legislation; (b) other proposed projects or developments of agencies; or (c) other proposed projects or developments of organisations?

As already noted in response to Q 4-35, we support a requirement for major personal information handling projects, in both the public and private sectors, to commission a privacy impact assessment, and, most importantly, for them to be made public as a contribution to debate, prior to irrevocable decisions to proceed. Experience from other jurisdictions where such a requirement is in force (e.g. the US federal government) can be drawn on to design appropriate threshold criteria for triggering the requirement.

6–7 If privacy impact assessments are required:

(a) who should be involved in preparing the assessments;
(b) who should be entitled to view the results of the assessments;
(c) who should bear the cost of the assessments; and
(d) what role should the Privacy Commissioner play in overseeing any requirements placed on agencies or organisations in this regard?

Privacy Impact Assessments could be undertaken either in-house, by the Privacy Commissioner, or by external consultants. There should be a presumption that they be made public. The cost should be borne by the proponent of the project. The Commissioner can play a number of roles, providing there is no direct conflict of interest.

6–8 Is the Personal Information Digest published in a useful manner? If not, how might it be improved? Is the record itself useful?

The Personal Information Digests (both Commonwealth and ACT) have not been used as effectively as they could be. They should provide a valuable research tool both for academic inquiry and for investigative journalism. However, now that the process is established, there is little marginal cost involved in agencies updating their entries, and web-publication by the Commissioner is also low-cost. The requirement should therefore be retained, in the hope that better use can be made of the Digests in future. The accessibility of the Digest should be improved to assist its use. It would be helpful to give the Commissioner greater discretion over the level of information to be provided in agencies annual returns, to allow more detail to be obtained in relation to significant information handling. If the Commissioner was authorised to grant any waivers from the basic requirements in IPP 5.3 for particular agencies or classes of agency, then this waiver should be subject to Parliamentary disallowance.

It is not appropriate for the Digest requirement to extend to the private sector generally, but consideration could be given to requiring very large businesses to prepare and publish a Digest entry - see our comment on the Openness Principles (IPP and NPP 5), under Chapter 4. The Commissioner could be empowered to selectively impose such a requirement.

6–9 What powers should the Privacy Commissioner have to audit agencies and organisations?

The audit power is very valuable – unfortunately resource cuts have limited the Commissioner's ability to undertake or commission audits in recent years. The audit power should extend to private sector organisations, where reliance on complaints to detect non-compliance is arguably even less effective than in the public sector. The Commissioner needs to be funded at a level that allows for a vigorous audit programme.

6–10 Should organisations and agencies be required to self-audit periodically to ensure and to demonstrate compliance with the *Privacy Act*?

Government agencies and larger private sector businesses should be required to either conduct internal audits of privacy compliance, or commission independent audits, and publish the audit findings. There may be some merit in exploring the potential for a relationship with Australian and international quality and other standards certification.

.

6–11 Should all the Privacy Commissioner's functions be consolidated in the *Privacy Act?*

It is helpful to list all of the Commissioner's functions in the Privacy Act (currently s.27) even where those functions are conferred by other legislation.

6–12 Are the procedures under the *Privacy Act* for making and pursuing a complaint, including a representative complaint, appropriate? Are the Privacy Commissioner's powers to make preliminary inquiries and investigate complaints appropriate and effective?

The complaints provisions of the Privacy Act contain some major weaknesses, although some of these could be mitigated by a different approach by the Commissioner to complaint handling. The problems can be summed up as:

- *Complaint handling is too slow and bureaucratic, and is often unresponsive to complainants' desired outcomes*
- *Successive Commissioners have been too conservative in their interpretation and use of their powers.*
- *Commissioners have not encouraged or used the potential of representative complaints*
- *The Commissioners have failed to make effective use of their powers to make Determinations, even when requested to do so by complainants.*
- *Determination power appears not to allow for the Commissioner to prescribe acceptable acts and practices*
- *Commissioners have not been transparent about their complaint handling processes and decision making criteria*
- *Commissioners have not reported adequately on the outcomes of complaints, leaving a large gap in the information available to the public and representative bodies about the way in which the Act may be of use to them.*

For a more detailed critique of the complaint handling under the Privacy Act, which we endorse, we refer to the submission by Professor Greenleaf to the Privacy Commissioner's 2004-05 Review of the private sector provisions (at http://www.privacy.gov.au/act/review/revsub47.pdf)

6–13 Is the obligation of the Privacy Commissioner to investigate a complaint about an act or practice that may interfere with the privacy of an individual appropriate, and is it administered effectively?

The obligation is appropriate but it is not administered effectively in that individual complainants are often dissatisfied by the Commissioner's reluctance to make a formal decision about whether there has been an interference, and representative complaints are not encouraged or given the attention they may deserve.

6–14 Is the power of the Privacy Commissioner to investigate an act or practice that may interfere with the privacy of an individual appropriate, and is it used effectively?

The power is appropriate but it is not used effectively in that individual complainants are often dissatisfied by the Commissioner's reluctance to make a formal decision about whether there has been an interference, and representative complaints are not encouraged or given the attention they may deserve.

6–15 Are the Privacy Commissioner's powers relating to the conduct of investigations appropriate and exercised effectively? For example, are the Commissioner's powers regarding: (a) appearances before the Commissioner; (b) conferences; (c) obtaining information and documents; (d) examining witnesses; (e) entering premises to gather information; (f) discussion of complaints with a Minister or other designated person; and (g) reports, appropriate and exercised effectively?

The Privacy Commissioner's powers relating to the conduct of investigations are generally appropriate but are not always exercised effectively. The preference to date for attempted conciliation, by means of exchanges of correspondence over lengthy periods, is very inefficient and ineffective. Given the Commissioner's reluctance to even consider the formal determination making power, many of the powers provided are rarely used.

6–16 Are the Privacy Commissioner's powers under the *Privacy Act* to make determinations appropriate and administered effectively?

The Determination making powers are potentially very powerful. For reasons which have never been properly explained, successive Commissioners have been very reluctant to use these powers, with only 8 s.52 determinations having been made in 17 years. We know that many complainants desire, more than anything else, a formal finding that the respondent has breached a privacy principle. Greater use of the determination making powers would also result in a body of public decisions which would be a valuable resource for educating both data users and the public about the application of the law, and which could if necessary be formally challenged in the courts.

There is a specific problem with the Determination power which was highlighted by the Commissioner's four Determinations in 2004 on the residential tenancy database run by TICA. The Commissioner found that she did not have the power to prescribe actions that should be taken by TICA to ensure continued compliance – only to rule that particular acts and practices were in breach. This leaves enforcement as a 'guessing game' – i.e. 'Practice X is in breach but try something else and if challenged again we will see if that complies – but we can't tell you to do Y.' While we think the Commissioner may have misinterpreted the extent of her powers, it is clearly desirable for s.52 to include expressly include an ability to prescribe acceptable acts and practices.

6–17 Are the *Privacy Act* provisions for enforcing determinations adequate and administered effectively?

It is unfortunate that individuals (or the Commissioner) would have to go through 'de novo' federal court proceedings to enforce a Determination, if an agency or organisation failed to comply with its terms. We understand that for constitutional reason, the Privacy Act had to be amended in the 1990s to remove the automatic registration of Commissioner's Determinations as orders of the court.

We would like to see the ALRC canvass alternative enforcement mechanisms, and review whether there is any constitutionally valid means of avoiding having to hold de-novo federal court proceedings if respondents fail to comply with the terms of a Commissioner's Determination . Given the very small number of s.52 determinations, there is no practical basis on which to form a view about the Commissioner's administration of enforcing Determinations, except that it is not clear if the Commissioner has even followed up on the few Determinations made to see if they have been complied with.

We submit that the Commissioner should be required to publicly report on compliance with Determinations made in previous years.

Complainants and respondents should have a right to merits review of the Commissioner's Determinations.

6–18 Are the Privacy Commissioner's powers under the *Privacy Act* to make public interest determinations, including temporary public interest determinations, appropriate and administered effectively?

The powers to make Public Interest Determinations (PIDs) and Temporary PIDs are generally appropriate but have not been used often. Where they have been used, they have necessarily involved significant consultation and delay. This is appropriate given that they have the effect of weakening the level of privacy protection – not something that should be done lightly, particularly as they are subject only to 'default' parliamentary approval (i.e. they take effect unless disallowed). The Commissioner needs to be mindful of the burden which detailed PID consultations about often very complex issues place on unfunded consumer organisations.

6–19 Are the *Privacy Act* provisions for obtaining injunctions adequate and effective?

The provision for the Commissioner, or any other person, to apply for an injunction is valuable. To our knowledge it has only been used once, by a private business in the Channel 7 v MEAA case.

We submit that the Commissioner should make greater use of the injunction power, both during complaint investigations and as a pro-active tool where interferences with privacy are brought to attention in other ways.

6–20 Are the *Privacy Act* provisions for approving privacy codes appropriate and effective? Are privacy codes an appropriate method of regulating and complying with the Act? Why have privacy codes been so little used? Should the Privacy Commissioner have the power, on his or her initiative, to develop and impose a binding code on organisations or agencies?

The provision for Codes of Practice is potentially useful. It is hardly surprising that it is been so little used as it involves a significant resource commitment from the Code proponent, but offers little benefit, especially given the late amendment in 2000 that made decisions of Code Adjudicators reviewable by the Privacy Commissioner. The only Code to date to include a separate Code Administrator – the General Insurance Information Privacy Code - dealt with only a handful of cases, at considerable overall expense, and was withdrawn in 2006.
Most of the other Codes registered or proposed to date do little more than reproduce the NPPs in sector-specific language – a limited benefit. The only Codes to date to add significant additional commitments are the Biometrics Code, and arguably the Market and Social Research Code.
It would be helpful to extend the Code provisions to apply to public sector agencies and IPPs (but note our preferred solution of a single set of principle, to which Code provisions should attach). This would for example allow the Biometrics Code to be enforced against any Commonwealth agencies adopting it (as they should).

Codes could prove useful in interpreting the application of privacy principles in the context of specific sectors or technologies, but applications are unlikely – it would therefore be useful if the Commissioner could initiate Code development.

6–21 Is the current compliance model used in the *Privacy Act* appropriate and effective to achieve the Act's purposes? If not, is that because of its content, its administration, or some other reason?

The current compliance model has serious flaws, partly due to the content and structure, but mainly due to its administration. One fundamental problem is that relying on complaints as the main enforcement mechanism is inherently inadequate for privacy compliance. It leaves entirely to chance the range of compliance issues that are brought to the Commissioner's attention and requires the office to devote resources to the arbitrary selection of complaints, rather than to known systemic compliance issues

.

If the Commissioner was able and willing to focus more attention on identifying systemic non-compliance – with complaints as only one input, then far-reaching changes could be effected across whole sectors of activity, benefiting thousands of individuals rather than just the few complainants.

It is in the nature of privacy compliance that many breaches of privacy principles will never come to the notice of affected individuals, at least in a form that they recognise as being amenable to Privacy Act complaints (even assuming a high level of awareness of the Act, which is probably unachievable). Even where individuals are aware of privacy breaches, the consequences may not warrant the substantial investment of time and effort required to pursue a complaint. The absence of complaints cannot be taken as any indication of satisfaction or compliance.

The Commissioner and NGOs, working better together, can easily identify the main areas of non-compliance such as widespread inadequacy of privacy notices, unexpected and unwelcome secondary uses and disclosures, and inadequate security. A combination of better use of

representative complaints, pro-active investigation, and use of the injunction power could rapidly achieve systemic change.

6–22 Does the range of remedies available to enforce rights and obligations created by the *Privacy Act* require expansion? For example, should the available remedies include any or all of the following for particular breaches of the Act:

(a) administrative penalties;
(b) enforceable undertakings or other coercive orders;
(c) remedies in the nature of damages;
(d) infringement notices;
(e) civil penalties;
(f) criminal sanctions?

A wider range of remedies and sanctions is desirable. Experience of other jurisdictions suggests that administrative penalties and infringement notices can be particularly effective. We note that both the Spam Act and Do Not Call Register Act include such provisions. If they are considered suitable for the specialised privacy breaches addressed by these Acts (which although widespread and irritating, rarely have serious consequences) then they should be available for the range of potentially serious breaches of privacy principles.

Criminal penalties have generally not been considered appropriate for most privacy breaches, other than for willful obstruction of the Privacy Commissioner's functions. However, they have been included in the Credit Reportng provisions (PA Pt IIIA), in Telecommunications legislation, including for breaches of non-disclosure principles equivalent to NPP 2 (TA Part.13), and in computer crimes legislation which supports the security principles. A more rational and consistent approach to the role of criminal sanctions in Privacy law is desirable.

7. Interaction, Fragmentation and Inconsistency in Privacy Regulation

7–1 Does the multi-layered regulation of personal information create any difficulties? For example, does the multi-layered regulation of personal information:

(a) cause an unjustified compliance burden;
(b) create problems for organisations that operate in more than one Australian state or territory;
(c) complicate the implementation of programs and services at a national level;
(d) raise any issues in relation to the existence of multiple privacy regulators in particular industry sectors and across the states and territories; or
(e) act as a barrier to the sharing of information between public sector agencies and private sector organisations?

The multi-layered and complex pattern of privacy regulation in Australia undesirable both for business and for individuals. Individuals in particular are frequently confused about jurisdiction, and often frustrated and deterred by the effort required to establish who can assist them with a privacy problem.

On the other hand, it would be undesirable for any of the current level of privacy protection to be lost in any rationalisation. Levelling up is desirable, levelling down unacceptable.
As already noted, we believe there is great value in having multiple privacy regulators – experience has shown that Privacy Commissioners administration of privacy laws can be disappointing, and having more than one regulator (ideally interpreting a common set of principles) is an important form of 'peer review' which can contribute to maintenance of high standards and pro-consumer focus
.
It is essential however that multiple privacy regulators establish a good working relationship, particularly in expeditiously referring complaints where appropriate, and avoiding duplication

in the use of inevitably scarce resources. Despite a longstanding liaison forum, the privacy regulators in Australia have not worked closely enough at a practical level.

7–2 Do any issues arise for organisations that provide contracted services involving personal information to Australian Government, state or territory agencies? For example:

(a) are privacy provisions in Australian Government, state or territory agency contracts contributing to inconsistency and fragmentation in privacy regulation;
(b) are the *Privacy Act* provisions relating to Commonwealth contractors appropriate and effective;
(c) do issues arise for Commonwealth contractors that are subject to the NPPs and the IPPs;
(d) do any issues arise for organisations that provide contracted services involving personal information to both Australian Government and state or territory agencies;
(e) is there a concern that organisations acting under a state or territory contract may not be required to adhere to the same privacy standards that are applicable to private sector organisations under the *Privacy Act*? If so, how should that concern be addressed?

A single 'highest common' set of principles, which we call for elsewhere, would immediately address some of these issues. Provisions relating to contractors are not sufficiently clear and comprehensive. Privacy clauses in contracts are often overly legalistic, purporting to cover all possibilities but all too often failing to clearly allocate responsibility and for practical compliance and liability for breaches. Privacy Commissioners also need to accept greater responsibility for establishing who is responsible for alleged breaches where there are complex contractual and other relationships – individuals should not be expected to work this out for themselves.

7–3 How should personal information held on residential tenancy databases be regulated? For example, should it be regulated under the *Privacy Act*, by a binding code, or in some other way?

The experience of the representative complaint against TICA, resulting in four s.52 Determinations in 2004, demonstrated the need for additional regulation of tenancy databases, and this has subsequently been supported by the inter-governmental working party.
We support the regulation of residential tenancy databases by making all operators subject to the Privacy Act, and by requiring the Commissioner to develop a binding Code of Practice.

7–4 Does the inconsistent use of terms and definitions under federal legislation that regulates the handling of personal information create any difficulties? If so, what are some examples of the difficulties created?

It would be helpful if Commonwealth legislation used terms such as consent consistently, and rationalised relevant references to personal information and personal affairs. However, amendment of the Freedom of Information Act to change personal affairs to personal information has had the undesirable consequence of allowing agencies to claim the personal information exemption more often, in circumstances where the information in question is clearly about the official business role of public servants. This has reduced accountability and discredits the privacy protection in the eyes of the public and the media. There may be a case for re-introducing a clear distinction between personal information and personal affairs in the context of disclosure limitations, while ensuring that individuals obtain the benefit of the wider definition in the context of other rights

.

7–5 Do any difficulties arise as a result of the interaction between the *Privacy Act* and provisions in other federal legislation that require or authorise acts or practices that would otherwise be regulated by the IPPs or the NPPs? If so, how should the interaction between the *Privacy Act* and these provisions be clarified?

Clarification of the relationship between the Privacy Act and other laws is desirable . We submit that a basic distinction should be made between other laws which <u>expressly require</u> particular uses and disclosures should form exceptions to the use and disclosure principles in the Privacy Act, but that where acts or practices are only 'authorised' then the use and disclosure principles

in the Privacy Act should prevent use and disclosure unless another exception applies i.e. mere lawful authority (which is understood to include common law and contractual authorities) should not in itself be grounds for use and disclosure for secondary purposes without consent.

7–6 Does the interaction between the *Privacy Act* and other federal legislation that regulates the handling of personal information require clarification? In particular:

(a) does the overlap of the *Privacy Act* and *Freedom of Information Act 1982* (Cth) provisions relating to access and amendment of records give rise to any difficulties;

Yes – the overlap is confusing both to the public and to the agencies with obligations under both Acts and should be rationalised – taking account of the useful recommendations of ALRC Report 77 in 1995, to which the government has yet to respond.

(b) should the *Privacy Act* provide for a process of consultation prior to granting access to information that includes personal information about a third party rather than rely on the process outlined in the *Freedom of Information Act 1982* (Cth);

We are indifferent to the location of these process requirements as long as they are reviewed in light of the ALRC Report 77 recommendations and subsequent experience.

(c) should the *Privacy Act* and the *Freedom of Information Act 1982* (Cth) be administered by the same body;

A Freedom of Information Commissioner is long overdue, as the FOI Act is no longer working as originally intended due to government neglect and outright resistance, and requires an independent champion. There are both advantages and disadvantages in co-locating administration of FOI and Privacy (as has been done in the UK and Canada).

(d) should the *Privacy Act* apply to certain classes of records in the open access period for the purposes of the *Archives Act 1983* (Cth);

We have not formed a view.

(e) should the exemption under the *Archives Act 1983* (Cth) relating to 'information relating to the personal affairs of any person' be amended to provide an exemption in relation to 'personal information' as defined in the *Privacy Act*;

See our response to Q 7-4

(f) should the *Privacy Act*, the *Freedom of Information Act 1982* (Cth) and the *Archives Act 1983* (Cth) be consolidated in one Act;

This is an over-ambitious idea and probably unnecessary. It is more important that all three Acts are reviewed and amended to ensure consistency and compatibility

.

(g) should federal legislation relating to the handling of tax file numbers and data-matching be consolidated in one Act? If so, should they be consolidated in the *Privacy Act*;

The tax file number guidelines are in need of major review in light of successive government extensions of the authorised uses, and of subsequent developments in data-matching and identity management. Some of the detailed requirements for consent no longer serve any useful purpose in the context of government decisions and probably only operate to individuals' disadvantage, thereby discrediting privacy law. The use of tax file numbers should be addressed partly in tax law and partly in a revised provisions of the Privacy Act dealing generically with government identifiers – see our responses to Chapter 4 in relation to NPP 7 and to Chapter 12.

The specific Data-matching legislation seems to be well established and compliance does not seem to be a problem. There seems no reason to change this law, other than as one way of extending the scope – see (h) below.

(h) should data-matching programs that fall outside the *Data-matching Program (Assistance and Tax) Act 1990* (Cth) be more formally regulated;

We support the recommendations of earlier inquiries that all Commonwealth data-matching should be subject to binding rules based on the Privacy Commissioner's Guidelines. We are indifferent to whether this is effected through the Data-matching or Privacy legislation, although the Privacy Commissioner's functions in the Privacy Act should be updated to reflect any change.

(i) is personal information collected pursuant to the *Census and Statistics Act 1905* (Cth) adequately protected;

We consistently drew attention during the 1990s to the Bureau of Statistics as the one and only Commonwealth agency which could give unqualified assurances of confidentiality. Regrettably this is no longer the case since the introduction in 2005 of the Longitudinal Data Set (albeit on a sample basis)[2], and in the last two censuses of the 'opt-in' retention of forms by the Australian Archives, for access by researchers after 99 years. Any further erosion of the confidentiality provisions of the Census and Statistics Act needs to be firmly resisted, not only because of the extraordinary sensitivity of much census information, but also because of the public interest in truthful and therefore reliable census responses. The recent 'emergencies' amendments to the Privacy Act almost inadvertently eroded the secrecy provisions and only the vigilance of the Bureau of Statistics ensured that this did not occur.

(j) is it appropriate that the disclosure of a shareholder's personal details in a register of members, register of debenture holders or a register of option holders under the *Corporations Act* is a disclosure of personal information that is permitted for the purposes of NPP 2;

This is a difficult issue as the accountability and market facilitation functions of public shareholding etc. registers inevitably limits the privacy of shareholders etc. The Corporations Act could usefully contain more specific restrictions on the purposes for which third parties can communicate with shareholders etc., using information obtained from public shareholder etc. registers.

(k) does the *Commonwealth Electoral Act 1918* (Cth) provide adequate protection of personal information included on the electoral roll;

No – successive amendments to the Electoral Act have turned the electoral roll into a resource for identity management, far removed from its original limited purpose of facilitating representative democracy. This is starkly illustrated in a recent publication by the Victorian Electoral Commission[3] and some of our criticisms of the Act are noted in summarised in our submission to a Senate Committee[4] Not only are disclosures contrary to the spirit of the Privacy Act, but information now required from individuals enrolling to vote have more to do with the other uses of the roll than with its primary purpose.

(l) does the Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 (Cth) adequately protect personal information?

No – the AML-CTF legislation, now passed, represents one of the most objectionable and disproportionate intrusion into financial privacy, as well as extending the existing

[2] See our submission at http://www.privacy.org.au/Papers/ABSCensusPIAresp050711.pdf
[3] *at http://www.vec.vic.gov.au/files/ElectoralEnrolmentInformationCollectionandDisclosurePractices.pdf*
[4] *at http://www.privacy.org.au/Papers/Sen-ElectIntegrity-0603.rtf*

system of highly subjective suspect transaction reports, which are exempt from access and correction rights. Our concerns about this legislation are detailed in our submission to the Senate Committee[5]

The unsatisfactory relationship between the Privacy Act and the Telecommunications Act 1997 is discussed in Chapter 10

7–7 Do the various secrecy provisions under federal legislation that prohibit individuals employed by the Commonwealth from disclosing information contribute to inconsistency and fragmentation in personal information privacy regulation? In particular, should the *Privacy Act,* rather than secrecy provisions in specific statutes, regulate the disclosure of personal information by Australian Government agencies?

It is appropriate for individual statutes to contain specific non-disclosure provisions. General provisions in the Privacy Act could never specify in sufficient detail the particular disclosure regimes which are appropriate for particular types of information and particular agencies. Any attempt to standardise non-disclosure provisions would inevitably contribute to a weakening of privacy protection based on a presumption that it is acceptable for governments to use information collected for a specific purpose for any other public purpose. We reject this presumption as fundamentally in conflict with the purpose specification and limitation objective of privacy law.

7–8 Are the provisions in Part VIII of the *Privacy Act* necessary? If so, are the provisions adequate and should they be contained in the *Privacy Act* or elsewhere?

Neither the objectives of Part VIII, nor the circumstances in which they might apply are clear. The law could usefully clarify this.

7–9 Do privacy rules, privacy codes and privacy guidelines developed under federal, state and territory legislation, or by organisations and industry groups, contribute to fragmentation and inconsistency in the regulation of personal information?

The wide range of privacy rules, privacy codes and privacy guidelines probably do contribute to fragmentation and inconsistency in the regulation of personal information but need not necessarily do so. With a simplified common set of principles and greater consistency between jurisdictions, there would still be a valuable role for sector or activity specific guidelines and codes.

8. Health Services and Research

8–1 Does the regulation of health information require a different and separate set of privacy principles to those used to regulate other sensitive personal information?

The basic set of information privacy principles should apply to health information and other sensitive information and we see no need for separate legislation. There is however a need for supplementary rules on the detailed application of the basic principles to the handling of personal information in a health context.

8–2 Should s 3 of the *Privacy Act* be amended to state that the Act is intended to regulate the handling of health information in the private sector to the exclusion of state and territory legislation?

This would be one approach to simplification, but may fall foul of constitutional limitations on the ability of the Commonwealth to legislate, for instance, for the actions of unincorporated

[5] at http://www.aph.gov.au/senate/committee/legcon_ctte/aml_ctf06/submissions/sub09.pdf

health professionals. The current proliferation of different rules and overlapping health privacy jurisdictions is in no-one's interest but the solution is not easy.

8–3 Is the draft *National Health Privacy Code* an effective way to achieve a nationally consistent and appropriate regime for the regulation of health information? If so, what is the most effective model for implementing the draft *National Health Privacy Code?* If not, what other model should be adopted to achieve a nationally consistent and appropriate regime for the regulation of health information?

In principle, a National Health Privacy Code could usefully form the basis of the more detailed supplementary principles which we believe should be adopted as a common standard in all Australian jurisdictions. However, there has been little public consultation on the current Health Privacy Code and we reserve our position on its content. One difficulty with the development of a separate code is that it encourages drafters and stakeholders to adjust the information privacy principles more than necessary, creating arbitrary or intricate differences that then create confusion. This is evident in the creation of the Health Records Act in Victoria, which adopts much of the information privacy principles that appeared in the State's Information Privacy Act but is more prescriptive and creates distinctions that may or may not be significant yet cause confusion. For example, the Health Records Act requires organisations in health privacy principle 1.3 to 'take steps that are reasonable in the circumstances to ensure that the individual is generally aware' about the purposes for which the information is collected. By contrast, information privacy principle 1.3 in the Information Privacy Act requires organisations to 'take reasonable steps to ensure the individual is aware' of the same things.

8–4 If the draft *National Health Privacy Code* is not implemented nationally, should the Australian Government adopt the Code as a schedule to the *Privacy Act*?

The answer to this question depends on the ability of the Commonwealth to cover the field to the exclusion of State and Territory laws (see Q 8-2). Unless it can do so, adopting the Code as a schedule to the Privacy Act would simply compound the existing confusion. We cannot comment further in the absence of an up to date publicly available version of the Code to discuss.

8–5 Do electronic health information systems require specific privacy controls over and above those provided in the *Privacy Act* or the draft *National Health Privacy Code*?

If there is appropriate regulation of data-matching and of the use of identifiers (both discussed elsewhere) together with improvements to the principles, then there should be no need for controls specific to electronic health record systems. However, the experience in NSW, where the government has overridden a very clear 'opt-in' rule for electronic health records (Health Privacy Principle 15) in order to trial the HealtheLink system, shows how easily apparent protection can be subverted.[6]

Moreover, it does not necessarily follow that, the creation of specific health privacy principles, in a separate code or in separate legislation,will strengthen the standards of protection available for health information compared to that available for non-health information. For example, the Health Records Act in Victoria allows greater data sharing of health information than is permitted for non-health information under the Information Privacy Act. Health information can be shared under Health Privacy Principle 2,2(f) for the very broad purpose of 'funding, management, planning, monitoring, improvement or evaluation of health services' if it is impracticable to seek consent or reasonable steps are taken to de-identify it. No equivalent exception exists for other personal information in Victoria.

8–6 The *National Health Act 1953* (Cth) requires the Privacy Commissioner to issue guidelines in relation to the handling of personal information collected in connection with claims under the Medicare Benefits Program and the Pharmaceutical Benefits Program. Is this an appropriate and effective role for the Privacy Commissioner?

[6] *See* http://www.privacy.org.au/Campaigns/E_Health_Record/HealthElink.html

This is a reasonable role for the Privacy Commissioner to play and Commissioner's recent consultation on the Guidelines[7] was a satisfactory although lengthy process, even though we did not agree with all of the findings.

8–7 Are the definitions of: (a) 'health information'; and (b) 'health service' in the draft *National Health Privacy Code* appropriate and effective? Should the *Privacy Act* be amended to adopt these definitions?

These are detailed issues on which we have not yet formed a view. Much depends on how the information caught by the broader definition will be protected. If by extending the definition, the information then falls under principles that provide less protection than the principles that currently protect non-health information, we would not support it. For example, we would oppose the inclusion of information about aged services if it effectively meant a reduction in privacy for all citizens over retirement age.

8–8 Should the *Privacy Act* be amended to ensure that all agencies and organisations that collect, hold or use health information are required to comply with the Act?

See our answers to questions 8-2 and 8-4.

8–9 Is guidance by the Office of the Privacy Commissioner to clarify that organisations can disclose health information for the management, funding and monitoring of a health service an appropriate and effective response to concerns in this area? If not, what is an appropriate and effective response?

We are concerned that management, funding and monitoring of health services are too broad concepts for an exception to the normal requirements for consent, express legal authority etc. Almost any activity could be encapsulated by these three terms, and they effectively allow governments to use detailed health information about individuals for a wider range of secondary purposes for which de-identified information should suffice.

8–10 Is there evidence that the regulation of personal health information impedes the provision of appropriate health services to individuals? If so, what changes are necessary to facilitate the provision of appropriate health services?

Despite many generalised allegations, we are not aware of specific examples of how regulation of personal health information has impeded the provision of appropriate health services to individuals. To the extent that example are forthcoming, these need to be balanced against the possible harm to both private and public health if individuals trust in the confidentiality of health information is undermined by unwelcome proliferation and secondary uses.

8–11 Does the *Privacy Act* provide an appropriate and effective regime for handling health information in those circumstances where an individual has limited capacity to give consent? Does the draft *National Health Privacy Code* provide a more appropriate and effective framework for handling health information in these circumstances?

These are detailed issues on which we have yet to form a view, and we will not comment without seeing a current version of the Code. We are not confident that the Code actually provides a higher standard of protection rather than facilitating the sharing of health information among government agencies. We are not convinced that the special requirements of the handling of health information could not be met by moderate amendments to the NPPs, which would also make it easier for holders of both non-health and health information to identify and understand the differences between how the different types of personal information should be handled..

[7] *see* http://www.privacy.gov.au/act/review/healthreview.html

8–12 Are there any other issues relating to consent to deal with health information in the health services context that the ALRC should consider?

None immediately apparent.

8–13 Should the *Privacy Act* be amended to allow health service providers to collect information about third parties without their consent in line with Public Interest Determinations 9 and 9A? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of such information than the current provisions of the *Privacy Act*?

These are detailed issues on which we have yet to form a view.

8–14 Should the *Privacy Act* be amended to allow insurance companies to collect health information about third parties without their consent in similar circumstances to those set out in Public Interest Determinations 9 and 9A?

These are detailed issues on which we have yet to form a view.

8–15 Should NPP 10 of the *Privacy Act* be amended to clarify when health information may be collected without consent? Does NHPP 1 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for collection of health information without consent? *This is a detailed issue on which we have yet to form a view.*

8–16 Are there any other issues relating to the collection of health information that the ALRC should consider?

Not at this stage.

8–17 Is guidance by the Office of the Privacy Commissioner an appropriate and effective response to concerns that the phrases in NPP 2, 'primary purpose of collection' and 'directly related to the primary purpose', might impede the appropriate management of an individual's health? If not, what is an appropriate and effective response?

There is no reason why health services should require special treatment in relation to interpretation of NPP 2. We comment on the primary/secondary purpose distinction in our response to Chapter 4, and the same combination of principle revision, Code development and Commissioner's guidance will be appropriate for all sectoral applications of a use and disclosure principle.

8–18 Does NHPP 2 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for the use and disclosure of health information than the current provisions of the *Privacy Act*?

This is a detailed issue on which we have yet to form a view.

8–19 Are there any other issues relating to the use and disclosure of health information that the ALRC should consider?

We have nothing to add at this stage

8–20 Is the exception in NPP 6.1(b) in relation to providing access to health information (that is, that access may be denied if it would pose a serious threat to the life or health of any person) appropriate and effective? Should the exception be extended to allow a health service provider to deny access to health information if providing access to the information would pose a threat to the therapeutic relationship between the health service provider and the health consumer?

We are not aware of any experience that would suggest a need for this exception to be changed. We would be very wary about any suggestion that the preservation of a relationship should

override an individual's right to see health information held about them, subject to the other accepted exceptions.

8–21 Do NHPP 6 and Part 5 of the draft *National Health Privacy Code* provide a more appropriate and effective framework for access to health information than the current provisions of the *Privacy Act*?

This is a detailed issue on which we have yet to form a view.

8–22 Should the *Privacy Act* be amended to deal expressly with the situation in which a health service provider ceases to operate? Does NHPP 10 of the draft *National Health Privacy Code* provide an appropriate and effective framework to deal with this situation?

There is a range of other circumstances e.g. financial advice, where the same issue arises . However, in many of those other circumstances the customer would normally routinely see some of the information e.g annual statements. This is not normally the case with health information. Individuals typically trust GPs or specialists as the sole custodians of health records.

So if a health professional's practice is going to close, there should be a requirement for contact with the information subject to give them a choice as to who the information should be transferred – not another practitioner chosen by the retiring professional.

There should also be a requirement that health information can be transferred at ANY time of the choosing of the patient to a new practitioner. Instances where that would be important are moving interstate, the death of the primary care physician within a group practice, and significant stage of life changes (e.g. child, adult, senior). We have not been able to consider NHPP 10 as a possible model for a generic solution.

.

8–23 Are there any other issues the ALRC should consider in relation to access to health information?

We have nothing to add at this stage.

8–24 Does NHPP 11 of the draft *National Health Privacy Code* provide a more appropriate and effective framework to deal with the transfer of health information from one health service provider to another than the current provisions of the *Privacy Act*?

We have not formed a view on this issue

.

8–25 Is the current public interest test in the *Privacy Act* and Section 95 and Section 95A Guidelines (that the public interest in promoting research substantially outweighs the public interest in maintaining the level of protection of health information provided by the Act) appropriate and effective? If not, what is an appropriate and effective test?

The current test seems appropriate and we not aware of any evidence that it has been problematic.However, see our response to Q 8-26.

8–26 Should the term 'research' be defined for the purposes of the *Privacy Act*? If so, how should the term be defined?

This is a generic question that should be dealt with outside the specific context of health information. We submit that it would be useful to draw a distinction between different modes of research.

Survey research which conforms to the Association of Market Survey and Research Organisations (AMSRO) Code of Practice, i.e. where the researchers keep the identity of research respondents or subjects confidential and do not reveal personal information to clients

(whether internal or external), clearly poses far fewer privacy risks, and can be given conditional exemption from some of the privacy principles.

In contrast, survey research which either by design or incidentally involves personal information about research subjects becoming known to the commissioning organisation and used for other purposes (whether commercial or not), carries with it a greater potential privacy risk, and should be subject to the principles in full.

Research can be of an entirely different character, not involving direct contact with respondents but instead accessing and using information collected for another primary purpose. In these circumstances, the research use should generally be subject to an even higher standard – of full and informed express consent.

All of these legitimate forms of research need to be distinguished from analysis for management and planning purposes, which is often misleadingly described as research. NPPs 2.1 (d) and 10.3(a) attempt to make this distinction, but without offering the differential protection that is required, and also without defining 'research' – this probably needs to be done to avoid self-serving interpretations.

8–27 Should the *Privacy Act* be amended to include definitions of 'identifiable', 're-identifiable' and 'non-identifiable' personal information?

This is a generic question which should not be confined to health research and should therefore be considered in one of the other chapters e.g. rather than specifically in the context of health information. Health researchers have constructed elaborate mechanisms to allow data linkage which provide a degree of protection but do not amount to de-identification. Information either is or is not actually or potentially identifiable The ALRC should be wary about legitimising the idea that there can be an intermediate category.

8–28 Should the *Privacy Act* draw a distinction between 'identifiable' and 're-identifiable' health information in the context of health and medical research?

As for Q 8-27 - This question is best answered generically rather than specifically in the context of health information. Health researchers have constructed elaborate mechanisms to allow data linkage which provide a degree of protection but do not amount to de-identification. Information either is or is not actually or potentially identifiable The ALRC should be wary about legitimising the idea that there can be an intermediate category.

8–29 What provision should be made for the use of health information without consent in health and medical research?

Medical or epidemiological researchers make a case for exemption from a consent requirement on the grounds that participation only by volunteers will bias their findings, and that the public interest in the value of their research outweighs privacy interests. The Act already deals with this 'special case' adequately by providing for health research without consent with specific approval from ethics committees.

8–30 Does NPP 2 provide an appropriate and effective framework for the use, without consent, of health information in health and medical research?

See our response to Q 8-29. There is no need for any special treatment of use without consent beyond the current provisions of NPP2.1(d), which should also apply to public sector use in any unified principles

.

8–31 Are Human Research Ethics Committees the most appropriate bodies to make decisions about the collection, use and disclosure, without consent, of health information in the context of health and medical research?

Human Research Ethics Committees seem entirely appropriate bodies to make these decisions and we are not aware of any evidence or experience to the contrary. It may be time consuming and frustrating for researchers, but it should not be 'easy' to get approval for collection use and disclosure without consent, if none of the other exceptions apply

.

8–32 Are the requirements imposed on Human Research Ethics Committees by the Section 95 and Section 95A Guidelines issued under the *Privacy Act* appropriate and effective?

We are not aware of any experience that suggests these requirements are not appropriate and effective.

8–33 Does the *Privacy Act* provide an appropriate and effective regime for: (a) the establishment of health data registers; and (b) the inclusion and linkage of health information in data registers? *See our response to Q 8-5 in relation to electronic health records. Registers or databases for non-clinical uses such as research should be able to operate under the current Privacy Act regime, subject to comments already made.*

9. Children, Young People and Adults with a Decision-Making Disability

9–1 Should the protection of personal information for children and young people be dealt with expressly in the *Privacy Act*? If so, how should the Act be amended? For example, are there privacy issues arising in the areas of:

- child welfare, juvenile justice or family law;
- disclosure of health information to parents;
- information held by schools and child care centres;
- online consumer information;
- taking and publishing photographs;
- broadcasting of identifying images and information; or
- identification of children and young people in court records.

No - It is not necessary for information about children and young people to be expressly dealt with in the Privacy Act. The Privacy Act already applies to both adults and children, and this helps ensure that children are afforded the same privacy rights and protections as adults.

The Act could however be amended to clarify that it does apply to all individuals, regardless of age.

We would support the development of more detailed guidelines (or similar non-legislative instrument) to support the Act to deal more effectively with the issue of consent, and when it may or may not be appropriate for parents/carers to consent on behalf of children.

We support children being able to make decisions regarding their personal information where they are deemed capable of making an informed decision. In most instances this is best determined on a case-by-case basis. Developing more detailed guidelines that could be used by organisations (such as schools and counsellors) when making decisions involving a child's personal information would improve consistency in this area without necessarily having to apply restrictive rules based around a particular age.

We would also support the general principle that, even where children are not deemed capable of informed decision-making, they should be involved where possible in any decisions made about them and their views considered.

There may be other legislation where it is necessary for the handling of personal information about children and young people to be dealt with expressly. For example, large-scale projects such as the Access Card deal with large amounts of personal information about children and young people, and may involve specific practices that need to be addressed.

In situations where an across-the-board age limit is proposed that affects when a child is able to make decisions about the handling of their own information, consultation would be required to determine the appropriate handling of information in the particular circumstances as this may vary given the nature of the information being considered.

In relation to some of the specific questions in 9-2:

Disclosure of health information to parents

Access Card proposal - We note the problems discussed in the ALRC Report on the contentious issue of the age at which children may have their own Medicare Card, and at what age the child's consent would be required for parents to access this information. These problems will multiply under the proposed Access Card scheme.

The proposal from the Access Card Office is that children under the 18 will not be issued with an Access Card, unless a special exemption is sought (and there is no lower age limit for this exemption). A number of competing privacy interests would need to be considered for younger children granted such an exemption. While these children would have their own Access Card, the question of parental access to the information on the card remains unclear. If parents are given access to information on their child's card, how will this be managed? Who controls the access to the information and makes such a decision? Also, because it is not longer simply a Medicare Card used for a single purpose, young children who do have their own Access Card granted by exemption will be subject in this sense to a more privacy invasive scheme that those who do not have one.

For children under 18 without an Access Card (that is, most of this population group), their health information may be more widely accessible than under the current Medicare scheme. This is because children are to be included on their parents cards, in many cases resulting in children's data being contained on more than one Access Card (eg the Card of both parents, foster parents etc). How this information will be updated and maintained is not yet clear. This scheme raises the age at which children are able to independently manage their own health information to 18, and may deter some children from seeking the health care they need (for example in relation to mental health, contraception or drug-related issues) if such information is available to their parents.

Clearly, proposals such as the Access Card scheme raise many complex questions about parental access to children's health information. We submit that more detailed consideration and consultation is required on these issues, and that they should be dealt with expressly in the Access Card legislation.

Information held by schools and child care centres

There are a number of other technologies other than those mentioned in the ALRC report that collect personal information about children. For example fingerprinting (in school libraries), swipe cards (to record and monitor attendance) and CCTV cameras (for security purposes) are used in some Australian schools and more extensively in other countries such as the UK. Some child care centres offer webcam technology to allow parents to view their children. Often these technologies are introduced for administrative convenience, with little regard for privacy concerns of the children involved. A system to

monitor and consult on such developments before they are introduced would help address important privacy issues.

Online consumer information

Children are at the forefront of use of new technologies for handling personal information. Not only is information about children being collected and used via new technologies at a greater rate than before, children are themselves high users of such technologies from an early age. Therefore, the issue of how information is exchanged and managed between and by individuals (not just organisations) is an important consideration. For example, in relation to children, information collected by peers or parents may raise privacy issues in some situations.

Updating privacy legislation to deal with exchanges of information between individuals online should be an important area of review.

Equally important is the need to raise awareness about privacy issues amongst both children and those who handle information about children. For example, in relation to children's use of websites, a large amount of personal information may be submitted by the child. While regulation of online providers and businesses in relation to the collection of information may provide some protection, legislation alone will not fully guarantee children's privacy protection. Education on privacy issues is also important, and we would support more widespread educative programs in this area.

Taking and publishing photographs

Organisations who take and/or publish photographs of children and young people must consider privacy implications, particularly in view of potential widespread dissemination via the web. Some organisations (such as schools and child care centres) develop their own privacy policy on the photographing of children within the organisation, but this is by no means consistently applied. We would support a more consistent approach by organisations and business on taking and publishing photographs, particularly of children.

Also, as noted earlier, children and young people are also high users of technology (for example, mobile phones, digital cameras and webcams) that allow them to take photographs of others, including their peers and family. It is quite possible that a child's privacy may be threatened by a disenchanted peer posting photographs on the web without the individual's consent. It is not clear how the Privacy Act would/could address such scenarios. A combination of legislation and education is likely to prove most successful.

9–2 Are there any other issues relating to the privacy protection of children and young people that are currently outside the scope of the *Privacy Act* that need to be addressed?

One issue is the increasing use of surveillance products by parents (not just organisations). For example, tracking devices (such as GPS devices in mobile phones, wrist watches or in track shoes) are increasingly being marketed as a method for keeping children safe. While there may be benefits from such technologies, they are generally introduced without discussion of the privacy issues. In these situations, the Privacy Act is of little assistance. This is because it is not always clear how the Act applies to surveillance practices, and also because it is the parent who uses the product and so the autonomy of the family prevails. There is no requirement for the companies developing the product to consider privacy issues if they are not themselves collecting personal information.

This point also highlights the fact that surveillance practices in a broader sense may not always be fully covered by the Privacy Act. For example, in situations where an individual is tracked, and personal information is not collected and stored in a record, the Privacy Act may not apply but the individual's privacy is nonetheless significantly affected.

9–3 Is there a need to amend the *Privacy Act* to facilitate better the protection of the personal information of adults with a decision-making disability? If so, what amendments are required? Are there any non-legislative options that should be adopted in relation to adults with a decision-making disability?

No – The Act should continue to apply equally to all individuals regardless of decision-making capacity.

However (as mentioned above in relation to children), more detailed guidelines on consent arrangements for adults with a decision-making disability would help to achieve greater consistency. Underpinning these ought to be the general principle that the individual's views must be considered as far as possible in relation to any decisions about their personal information.

There are many different scenarios relating to individual decision-making capacity which need to be considered. For example, for some individuals, decision-making capacity may be restricted on an ongoing basis, while for others (such as with some mental illnesses) the inability to make fully informed decisions may occur more episodically. Similarly, the variation in decision-making capacity is enormous, thereby lending support to a case-by-case approach where possible.

10. Telecommunications Privacy

10–1 Do the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) provide adequate and effective protection for the use, disclosure and storage of personal information?

Regulation of privacy in telecommunications is a mess. It has relied too much on marginal changes to legacy 'non-disclosure' provisions from earlier telecommunications legislation. Weaknesses in the Privacy Act have been addressed by complex and onerous specific legislation (the Spam and Do No Call Register Acts) rather than by the sensible alternative of 'fixing' the Privacy Act. Many telecommunications privacy issues (such as calling number display, directories and silent lines) need rules covering both telecommunications providers and end-users, which has not been possible under telecommunications legislation alone.

10–2 What issues, if any, are raised by the interaction between the *Privacy Act* and the following Acts:

- *Telecommunications Act 1997* (Cth);
- *Telecommunications (Interception and Access) Act 1979* (Cth);
- *Spam Act 2003* (Cth);
- *Do Not Call Register Act 2006* (Cth)?

Are there acts and practices regulated by these Acts that would be dealt with better under the *Privacy Act*?

See our responses to Qs 10-1 and 10.3. For both data users and individuals, the relationship between these laws is confused. This has paradoxically led to one benefit in that the Telecommunications Industry Ombudsman has an overlapping jurisdiction in telecommunications privacy. The TIO with its much more consumer focussed complaint handling processes has therefore been able to handle some privacy complaints much more quickly, and probably more effectively, than if they had gone to the Privacy Commissioner. However, the

level of co-operation between the TIO and the PCO could be improved, particularly in addressing systemic policy issues.

A particular area of concern is the limitation on jurisdiction of Telecommunications legislation. Sensible approaches to privacy issues in telecommunications often involve regulation both of telecommunications businesses (telcos) and other businesses, such as directory producers and end-users of telecommunications. Several of the binding Codes developed by the industry body ACIF (now Communications Alliance) have been artificially limited in their scope by this jurisdictional constraints. For example, the Calling Number Display (CND) Code could only promote voluntary guidelines for use of CND by call recipients, and the Integrated Public Number Database (IPND) Code is apparently unable to regulate the activities of the IPND Manager – a key participant.- a similar limitation on coverage of directory producers had to be removed by the declaration of a new section of the Telecommunications Industry. It should not be necessary to have to resort to Declarations to regulate activities which cross the borders of an arbitrary concept of telecommunications.

The use of Codes under the Telecommunications Act has not generally been successful – their development takes an enormous amount of time[8] and under-resourced consumer groups struggle to make their voice heard in processes designed by and for industry participants. Once approved, adoption is voluntary unless they have been registered by the ACMA, and many Codes have not been signed by major telcos. Even registered, and therefore mandatory, Codes are not actively enforced.

Where the Code development process has been found wanting – as recently with the IPND – the alternative of direct legislation has been botched, with the IPND Act 2006 leaving a gaping hole by not regulating the directory activities of Telstra's Sensis subsidiary, which does not source its directories from the IPND. The strict rules applying to other directory producers do not apply to Sensis, leaving an uneven playing field and huge gaps in the protection offered to individuals.

The Issues Paper suggests (para 10.24) that NPP2 does not apply to telcos, on the basis that it is supplanted by Part 13 of the Telecommunications Act. We submit that this is an oversimplification and that NPP 2 can still apply. This needs to be clarified.

As the Issues Paper recognizes (para 10.29-10.30) , there is currently a regulatory gap in that small business operators in telecommunications are subject only to the TA but not also the PA, as larger businesses are. If a small business exemption is to remain, we endorse the recommendation of the Privacy Commissioner that all telcos be brought under the TA by Regulation, but this is very much a second best option which does nothing to address the arbitrary definition of telco already discussed.

As noted in the Issues paper (10.24 and on), there are inconsistencies in the limits on use and disclosure as between NPP 2 and Part 13. In some respects the PA is stronger than the TA and in other respects vice versa. There should be consistency unless a difference can be clearly justified.

There are particular major inconsistencies in the approach taken to consent for secondary uses, as between Telecommunications and Privacy law, but also within Telecommunications law. Some uses require positive consent (opt-in) (e.g. Spam Act) whereas others require only an opt-out opportunity (Do Not Call Register, Calling Number Display). The issues have already been discussed in relation to the direct marketing exception to the non-disclosure principle (see our response to Q 4-12). We noted there that the Spam Act works in practice more as an opt-out regime in relation to most of the Australian organizations likely to be involved in direct marketing to individuals. A more rational and consistent approach to consent within telecommunications law is desirable.

[8] The APF alone has logged an average of 35 hours a year on direct unpaid participation in ACIF processes over the last four years, leaving aside time spent preparing submissions on Codes and Guidelines and other telecommunications related work.

A particular factor in communications privacy is the exceptional interest shown by law enforcement and intelligence agencies in access to communications data, including content. There have been major extensions in the access powers of these agencies under Interception legislation. Special privileges have been given to these agencies under both Interception and general telecommunications laws without, in our view, adequate public debate about the appropriate balance between privacy and other public and private interests. Even the Privacy Commissioner has been excluded from the deliberations of the ACMA Law Enforcement Advisory Committee (and its ACA predecessor) which both develops proposals for future legal changes and advises on practical implementation of current laws. We submit that the Telecommunications Act should expressly require the Privacy Commissioner to be consulted, preferably through membership of this forum.

Our views in relation to the Telecommunications Interception have been documented in successive submissions on amendments to the interception legislation.[9] The overall picture has been of progressive weakening of the controls on interception, although a number of excellent official reviews[10] have put a brake on some of the more intrusive proposals.

We note that contrary to the suggestion at par 10.40, the Privacy Act IPPs do still apply to personal information obtained by most Commonwealth agencies under the Telecommunications (Interception and Access) Act 1979.

A valuable amendment to the Telecommunications (Interception and Access) Act 1979 in 2006 clarified the requirement for awareness for participant monitoring of communications to be lawful. However, this requirement is not widely understood and we submit that the Privacy Commissioner should be funded to undertake an education campaign aimed at businesses, and to enforce the requirement, breach of which may result in unlawful collection, also breaching NPP 1.

10–3 What bodies (public or private) should be involved in the regulation of personal information in the telecommunications industry?

A wide range of bodies have an interest in not just telecommunications but communications privacy generally – there should in principle be an equivalence between laws applying to postal and other delivery services, and telecommunications. The Discussion Paper could usefully canvass a fundamental re-appraisal of the balance between privacy and other public and private interests in communications.

The regulatory roles of the ACMA, the TIO and the Privacy Commissioner, as well as the Communications Alliance (in respect of Codes) and the ACCC, need to be clarified and relationships strengthened.

11. Developing Technology

11–1 What new technologies, or new uses of existing technologies, will, in the future, impact significantly on privacy? How can such technologies be accommodated in a regulatory framework?

It is impossible to predict technological change or the new government and business services that will take advantage of them. Privacy laws therefore need to be as 'technology neutral' as possible so that the objective of the principles are satisfied irrespective of the medium or channel used. At the same time, some technologies are known to raise particular issues (such as VoIP, RFID and so-called geo-identification), and it may be appropriate to address these specifically as they arise, either by amendment of the law, or through Codes of Practice and Guidelines.

[9] most recently at http://www.vec.vic.gov.au/files/ElectoralEnrolmentInformationCollectionandDisclosurePractices.pdf
[10] Most recently the Blunn Report cited in the Issues Paper (para 10.41)

11–2 Should the *Privacy Act* be extended to cover: (a) any acts or practices of individuals relating to their personal, family or household affairs; or (b) exempt agencies or organisations that use certain types of technology or collect certain types of personal information?

In relation to personal use, see our response to Q 5-1. There should be no exemption for any particular types of technology – rather, the law needs to ensure that the use of particular technologies does not escape from the requirements to comply with privacy principles.

11–3 Is there a need to amend the *Privacy Act* in light of technological developments? If so, what amendments are required? For example:

(a) should there be any additional limits on the collection of personal information;

It should not be necessary to have technology specific collection limitations.

(b) should agencies or organisations be required to obtain consent before using certain technologies to collect personal information? If so, should it be possible to refuse consent without any adverse consequences;

It should not be necessary to have technology specific requirements. The overall operation of privacy principles should give individuals as much choice as possible – see our response to Q 4-35 in relation to 'prevention of harm' and 'no disadvantage' principles.

(c) should biometric information be included in the definition of 'sensitive information';

Yes – biometric information should be included in the definition of 'sensitive information', but see our response to Q 3-4.

(d) should agencies or organisations be required to advise individuals of any misuse, loss or unauthorised access, modification or disclosure of personal information?

Yes – see our response to Q 4-35

Additional submission

Technologies that involve continuous monitoring, such as CCTV, tracking devices and computer logs, raise additional issues, as even if individuals have been informed at some point, they are likely to forget and/or relax their guard – there is no clear decision point, as there is in most other collection of personal information, at which individuals can make an informed decision. Such forms of surveillance are particularly insidious. This has been recognized to some extent in the passage of specific surveillance legislation in many jurisdictions, but it may be that some additional safeguards are needed as well in general privacy law to apply to the records resulting from surveillance. See our response concerning collection by observation to Q 4-3, and additional submission on the scope of the Inquiry in response to Chapter 1.

11–4 Should the *Privacy Act* be technologically neutral?

Yes, as far as possible, see our response to Q.11-1

11–5 What issues are raised by the publication in electronic form of publicly available records such as public records, court records and media reports? Does the *Privacy Act* need to be amended in response to these issues?

This is a complex area of competing public interests. There is no doubt that technological changes continue to affect the ease with which public records can be used for secondary and

often unexpected and unwelcome purposes. The collection, use and disclosure principles should apply to publicly available information to the maximum extent possible, preferably by reference to 'reasonable expectations' and 'public interest' tests. Despite the difficulties of enforcement, the law should challenge the entrenched idea that once personal information is in the public domain it should be available for any use.

12. Unique Multi-Purpose Identifiers

12–1 Are the schemes that regulate Tax File Numbers appropriate and effective?

See our response to Q 7-6 (g)

12–2 What unique multi-purpose identifiers are currently in use in Australia? What are the benefits and privacy concerns of using unique multi-purpose identifiers in transactions with agencies or organisations?

The use of identifiers can bring valuable benefits to individuals and efficiencies to business and government. However, the use of multi-purpose identifiers conflicts fundamentally with the purpose specification and limitation underpinnings of the privacy principles, and can facilitate major privacy breaches and compound the damage resulting from identity crime.

The proposed federal government Access Card (in effect a national identification scheme) is a particularly dangerous example of the use of multi-purpose identifiers and the fact that it can apparently be introduced consistently with the Privacy Act is a major indictment of the inadequacy of the Act. See http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html for our detailed comments on the Access Card.

12–3 What role, if any, should the *Privacy Act* play in the regulation of unique multi-purpose identifiers?

Privacy law should re-affirm the underlying purpose specification and limitation principles and generally discourage the use of multi-purpose identifiers. Where data linkage is justified, it is best to follow a multi-stage process of linkage with consent, or where expressly authorised by law, with separate identifiers for separate relationships. Tables of concordance between different identifiers can then be specifically authorised for particular purposes, with strict limits on use.

It is particularly important to maintain separation (silos) between areas of private life which are potentially sensitive – such as health care, financial affairs, movements and communications. Privacy law should aim to place significant barriers in the path of government or commercial initiatives which lead to personal information crossing these boundaries without express, free and informed consent.

13. Transborder Data Protection

13–1 Does NPP 9 provide adequate and appropriate protection for personal information transferred from Australia to a foreign country? Does the relationship between NPP 2 (disclosure of personal information) and NPP 9 (international transfer of personal information) need to be clarified?

See our response to Q 4-31. The regulation of transborder data transfers is currently inadequate, and the government has admitted that the Privacy Act does not provide enforceable remedies in the event, for instance, of breaches of privacy by offshore contractors.

13–2 Should the *Privacy Act* be amended to clarify that NPP 9 applies when personal information is transferred outside Australia to a related body corporate?

We understood this to already be the case – s.13B refers only to 'disclosure' as used in NPP 2, and not also to 'transfer' as used in NPP9. If this is unclear then it should be made express.

13–3 What role, if any, should the Office of the Privacy Commissioner play in identifying countries that have equivalent *Privacy Act* protection for personal information?

We submit that the Privacy Commissioner could usefully offer guidance on which overseas countries have equivalent privacy protection. The Commissioner may at any time have to form a view in the context of a specific complaint about a breach of NPP 9, and it would assist both business compliance and consumer choice to know in advance which jurisdictions posed a risk and where alternative arrangements would need to be made for protection. The Commissioner would be assisted in assessing overseas jurisdictions by the work of the EU Article 29 Working Party.

13–4 Should organisations be required to inform individuals that their personal information is to be transferred outside Australia? If so, what form should such notification take?

There should be a requirement to inform individuals that their personal information is to be transferred to any jurisdiction without equivalent privacy protection (including some State jurisdictions within Australia). Furthermore, there should also be a requirement to inform individuals to which jurisdiction(s) their personal information is to be transferred. so that individuals can exercise informed choice and/or bring pressure to bear for improvements in legislative protection.

13–5 Is adequacy of the *Privacy Act* under the European Union Data Protection Directive: (a) necessary for the effective conduct of business with European Union members; and (b) desirable for the effective protection of personal information transferred into and out of Australia? If so, what measures are necessary to ensure the adequacy of Australia's privacy regime under the European Union Data Protection Directive?

Businesses seem to be able to carry out business internationally without Australia receiving an adequacy assessment, but this is probably because of a lack of enforcement by EU regulators. Without an adequacy assessment, Australia runs the risk of having trade barriers imposed, and in any case it is desirable for Australian law to at least meet the EU standard of best practice.

13–6 Does the APEC Privacy Framework provide an appropriate model for the protection of personal information transferred between countries? Are other standards, such as the Asia-Pacific Charter, a more appropriate model?

The APEC Privacy Framework provides a bare minimum entry level 'floor' of information privacy protection, aimed at those jurisdictions without an existing higher level. APEC repeatedly emphasised that the Framework is not intended to weaken the level of privacy protection already provided by domestic laws in any member economy.

APEC is still working on the way in which the Framework might be used in the context of cross border data transfers, so it does not yet provide a model that can be assessed.

We submit that Principle 12 of the Asia-Pacific Privacy Charter provides an appropriate model for a revised transborder data flow principle.