National Legal Aid Secretariat
GPO Box 9898
Hobart TAS 7001

Executive Officer: Louise Smith

t: 03 6236 3813
f: 03 6236 3811
m: 0419 350 065

e: louise.smith@legalaid.tas.gov.au

National Legal Aid

Executive Director
Australian Law Reform Commission
GPO Box 3708
SYDNEY NSW 2001

21st December 2007

Dear Sir,

Re: NLA Submission to Australian Law Reform Commission Discussion Paper 72, Review of Australian Privacy Law

About National Legal Aid (NLA)

National Legal Aid (NLA) represents the Directors of the Legal Aid Commissions of all Australian states and territories. Legal Aid Commissions provide legal services to socially and economically disadvantaged people. The legal services we deliver involve representing clients who are eligible for legal assistance in federal, and state and territory courts and tribunals, the provision of dispute resolution services as appropriate, and the provision of information, advice, assistance and education to members of the public.

NLA aims to ensure the protection or assertion of the legal rights of people are not prejudiced by reason of their inability to:

- obtain access to independent legal advice
- afford the financial cost of appropriate legal representation
- obtain access to the federal and state and territory legal systems
- obtain adequate information about the law and the legal systems.

Australia's Legal Aid Commissions have a number of reasons to be interested in privacy legislation. We are particularly aware of the impact that information practices that lack privacy protection can have on our clients. For example, clients and their families are frequently on the receiving end of unfavourable publicity as a result of their involvement in the justice process.

We also accumulate extensive files on behalf of our clients containing highly sensitive information and are sometimes required to share information with other Commonwealth, state and territory agencies. We have an interest in promoting research into areas of crime and disadvantage. We work with community partners, particularly private lawyers and the community legal sector and this gives rise to concerns over the lack of privacy regulation for small business.

In approaching the Discussion Paper we have limited our responses to those issues which impact on the interests discussed above. We have tried to identify some of the implications of the interactions between recommendations contained in the Discussion Paper. For instance the recommendations to extend the Privacy Act to small business and for greater uniformity between Commonwealth, state and territory privacy regulation have implication for some of the proposals we discuss.

Protocols for special groups (proposal 1-1)

The Office of the Privacy Commissioner should, either on its own motion or where approached in appropriate cases, encourage and assist agencies and organisations, in conjunction with Indigenous and other ethnic groups in Australia, to create publicly available protocols that adequately respond to the particular privacy needs of those groups

We consider there is merit in this proposal which is consistent with initiatives that Legal Aid Commissions have taken or participated in to address the legal needs of specific groups. At the same time we should be cautious to avoid facile assumptions that indigenous people and other cultural minorities have collectivist values that place greater emphasis on group identity and less emphasis on individual privacy. This is not our experience. While information privacy supports the ability of individuals to control the flow of information about themselves, cultural differences will sometimes dictate different

priorities on how to exercise this kind of control. Consultation over such protocols therefore should be broadly based so as to reflect the diversity of views within any given group.

Proposal 3–2 The Privacy Act should be amended to achieve greater logical consistency, simplicity and clarity. For example, the Information Privacy Principles and the National Privacy Principles should be consolidated into a set of UPPs; the exemptions should be clarified and grouped together in a separate part of the Act; and the Act should be restructured and renumbered.

We support this proposal.

Definition of personal information (proposal 3-5)

The Privacy Act should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

We support a definition of personal information that more realistically reflects the relative ease with which as a result of recent advances in on-line services, an individual can be identified by people or organisations that have access to other data. This would remedy the unsatisfactory approach to identifiable information taken by the Victorian *Information Privacy Act* in *WL v LaTrobe University* [2005] VCAT 2592.

Coverage of deceased people (proposals 3-11 to 3-13)

The Privacy Act should be amended to include a new Part dealing with the personal information of individuals who have been dead for 30 years or less

The proposed provisions dealing with the use or disclosure of personal information of deceased individuals should make clear that it is reasonable for an organisation to use or disclose genetic information to a genetic relative of a deceased person to lessen or prevent a serious threat to the life, health or safety of a genetic relative.

Breach of the proposed provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the Privacy Act. The following individuals should have standing to lodge a complaint with the Privacy Commissioner alleging an interference with the privacy of a deceased individual:

(a) in relation to an alleged breach of the use and disclosure, data quality or data security provisions, the deceased individual's parent, child or sibling who is at least 18 years old, spouse, de facto partner or legal personal representative;

(b) in relation to an alleged breach of the access provision, any person who has made a request for access to the personal information of a deceased individual.

According privacy rights to deceased people raises complex issues that ought to be addressed at a more detailed level than simply broadening the definition of personal information to include those who have been dead for a limited period. Accordingly we support the proposal for dealing with this issue under a separate part of the Act. The proposed part should give explicit guidance on the need to balance the legitimate interests of survivors against the fact that deceased people are no longer able to make decisions about the way information is handled. The draft proposed in the Discussion Paper recognizes the need for balance by requiring organisations to apply a reasonableness test to decisions they make about information about deceased people. Given the tendency of many organisations to adopt an overly cautious approach to such reasonableness tests under existing privacy legislation, the legislation should include or mandate guidance to promote a more robust and realistic approach.

Interrelationship between Privacy Act and State and Territory laws.

Proposal 4-1 The Privacy Act should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

(a) Health Records and Information Privacy Act 2002 (NSW);

(b) Health Records Act 2001 (Vic);

(c) Health Records (Privacy and Access) Act 1997 (ACT); and

(d) any other laws prescribed in the regulations.

Proposal 4-2 States and territories with information privacy legislation that purports to apply to private sector organisations should amend that legislation so that it is no longer expressed to apply to private sector organisations.

Proposal 4-3 The Privacy Act should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'non-excluded matters' set out in the legislation. The Australian Government, in consultation with state and territory governments, should develop a list of 'non-excluded matters', for example matters such as:

(a) reporting for child protection purposes;

(b) reporting for public health purposes; and

(c) the handling of personal information by state and territory government contractors.

Proposal 4-4 The states and territories should enact legislation that regulates the handling of personal information in that state or territory's public sector that:

(a) applies the proposed Unified Privacy Principles (UPPs) and the proposed Privacy (Health Information) Regulations as in force under the Privacy Act from time to time; and

(b) includes at a minimum:

(i) relevant definitions used in the Privacy Act (including 'personal information', 'sensitive information' and 'health information');

(ii) provisions allowing public interest determinations and temporary public interest determinations;

(iii) provisions relating to state and territory incorporated bodies (including statutory corporations);

(iv) provisions relating to state and territory government contracts; and

(v) provisions relating to data breach notification.

The legislation also should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

Proposal 4-5 The Australian Government should initiate a review in five years to consider whether the proposed Commonwealth-state cooperative scheme has been effective in achieving national consistency. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy in the state and territory public sectors.

We support in principle the proposal for more consistent Commonwealth and State legislation. However, such proposals ought not to underestimate the complex issues surrounding any attempt to use Commonwealth legislation to cover the field, where laws on handling information are concerned.

Such laws are not limited to those that specifically protect personal information. They include other laws which protect different confidentiality interests, for example confidentiality provisions in state legislation that apply to specific classes of health information such as infectious diseases or disclosures by health sector employees that should not be overridden. State laws that protect the identity of people involved in court proceedings raise similar concerns. Child protection is covered by both Commonwealth and state laws.

As state bodies that provide legal services to clients who are in conflict with other branches of Government, Legal Aid Commissions are covered by legal provisions designed to ensure high levels of confidentiality for the information we use to administer legal aid schemes and assist individual clients. These laws supplement obligations of professional confidentiality and legal

professional privilege. We could not perform our functions if these restrictions were diluted to the extent of requiring or allowing such information to be freely disclosed for law enforcement and revenue protection purposes.

Action for breach of privacy (proposals 5-1 to 5-5)

The Privacy Act should be amended to provide for a statutory cause of action for invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, an invasion of privacy may occur where:

(a) there has been an interference with an individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

(d) sensitive facts relating to an individual's private life have been disclosed.

The Privacy Act should provide that, in determining what is considered 'private' for the purpose of establishing liability under the proposed statutory cause of action, a plaintiff must show that in all the circumstances:

(a) there is a reasonable expectation of privacy; and

(b) the act complained of is sufficiently serious to cause substantial offence to a person of ordinary sensibilities.

The Privacy Act should provide that:

(a) only natural persons should be allowed to bring an action under the Privacy Act for invasion of privacy;

(b) the action is actionable without proof of damage; and

(c) the action is restricted to intentional or reckless acts on the part of the defendant.

The range of defences to the proposed statutory cause of action for invasion of privacy provided for in the Privacy Act should be listed exhaustively. The defences should include that the:

(a) act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(b) act or conduct was required or specifically authorised by or under law;

(c) information disclosed was a matter of public interest or was a fair comment on a matter of public interest; or

(d) disclosure of the information was, under the law of defamation, privileged.

To address an invasion of privacy, the court should be empowered by the Privacy Act to choose the remedy that is most appropriate in all the circumstances, free from the jurisdictional constraints that may apply to that remedy in the general law.

Until such time as the states and territories enact uniform legislation, the state and territory public sectors should be subject to the proposed statutory cause of action for invasion of privacy in the Privacy Act.

We support the proposal for a limited statutory action. We agree that such an action should be limited to natural persons, so as to maintain consistency with information privacy legislation and the public accountability of corporate organisations. However for less well resourced parties it is important that the proposal incorporates alternative dispute resolution remedies.

Legal Aid NSW has already made a submission on the similar reference currently being conducted by the New South Wales Law Reform Commission. In that submission the threshold of reasonable expectation of privacy was questioned, as experience in the United States suggests that this relies on an excessively subjective assessment by courts and can turn into a continuously moving target as new information technologies gain acceptance.

Technological neutrality (proposal 7-1 to 7-2)

The Privacy Act should be technologically neutral.

The Privacy Act should be amended to empower the Minister responsible for the Privacy Act, in consultation with the Office of the Privacy Commissioner, to determine which privacy and security standards for relevant technologies should be mandated by legislative instrument.

Before making final recommendations on whether privacy laws should be expressed as technologically neutral, the Law Reform Commission would do well to consider just what this means in practice. Recent commentators have pointed out that the concept of technological neutrality can be ambiguous and suggested that technology specific regulation may be more appropriate for new forms of technology, where the outcome of a particular regulatory approach is uncertain. (Read 2007). We have concerns with the recommendation to adopt enforceable standards in proposal 7-2, to the extent that it could impose a degree or rigidity on a rapidly changing technological environment. It is useful to identify standards that can be used to determine whether specific conduct measures up to privacy requirements of reasonableness and or practicality, but this should not require that they be prescribed as part of the law.

Privacy invasive Internet Content Question 8–1

Should the online content regulation scheme set out in the Broadcasting Services Act 1992 (Cth), and in particular the ability to issue take down notices, be expanded beyond the National Classification Code and decisions of the Classification Board to cover a wider range of content that may constitute an invasion of an individual's privacy? If so, what criteria should be used to determine when a take down notice should be issued? What is the appropriate body to deal with a complaint and issue the take down notice?

We would give qualified support for such a proposal, given the lack of cost effective remedies for people who are unfairly represented on Internet sites but are unable to make use of the current *Broadcasting Services Act* provisions. Our reservations relate to the restrictions on free expression which are inherent on the current provisions of the Act and would be aggravated by a proposed extension to personal information that someone objects to being published. Regulation of objectionable content is primarily aimed at large scale or commercial dissemination of entertainment including pornography. Regulation of personal information would be more likely to impact on on-line journalism and personal websites, hence the more significant and subtle threat to free expression.

Expanding or duplicating the current regulatory regime for on-line content would also risk duplicating, and in some contexts expanding existing forms of privacy regulation. On balance, it may be more appropriate to give the Privacy Commissioner the power to issue a take down order to a service provider where a website has breached a provision of the Privacy Act or contains information that results from such a breach. Courts hearing matters under the proposed breach of privacy action could be given similar powers.

Definitions of contracted service provider and state contract

(Question 11-1) *Are the definitions of 'contracted service provider' and 'State contract' under the Privacy Act adequate? For example, do they cover all the types of activities that organisations might perform on behalf of agencies?*

The current provisions cause confusion to the extent that they create an arbitrary and somewhat artificial distinction between the way Governments contract with organisations to provide government services and fund organisations to provide services that benefit the community. The growing

trend for Governments to provide services through other organisations often gives rise to uncertainty as to which side of the line a particular service falls.

Where these services involve the performance of legal work it is important to maintain the distinction between an organisation that acts as an agent or provides independent professional services. The services we provide as Legal Aid Commissions are funded by both the Commonwealth and state and territory governments. In turn we fund or provide services through community partners, some of who may be contracted service providers as a result of agreements they have with other Government agencies. In making agreements to cover the provision of these services, we aim to ensure high standards of personal privacy when entering into agreements for the provision of services. It is not always clear how this is best achieved, having regard to uncertainties over the breadth of contracted service provider provisions.

We would hope that the adoption of other proposals in the Discussion Paper for more uniform privacy legislation and for removing exemptions for the definition of organisations would remove some of the complexities to which this question refers. In this way the question whether an organisation was a contracted service provider to the Commonwealth, a state or territory would cease to be the critical determinant of whether the privacy of its clients was secured.

Inter-jurisdictional information sharing for law enforcement (proposal 11-4)

The Australian Government, in consultation with: state and territory governments, intelligence agencies, law enforcement agencies, and accountability bodies (including the Office of the Privacy Commissioner; the Inspector-General of Intelligence and Security; the Australian Commission for Law Enforcement Integrity; state and territory privacy commissioners and agencies with responsibility for privacy regulation; and federal, state and territory ombudsmen), should:

(a) develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

(b) develop memoranda of understanding to ensure that accountability bodies can oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies

We support the proposal for appropriate privacy oversight of inter-jurisdictional sharing of personal information for law enforcement. Current arrangements

sometimes result in a blurring of accountability. This can be a particular concern where sharing of sensitive information affects people's liberty and reputation.

Accessing personal information held by agencies under Privacy Act (proposal 12-7)

The Freedom of Information Act 1982 (Cth) should be amended to:

(a) provide that an individual's right to access or correct his or her own personal information is dealt with under the Privacy Act; and

(b) repeal Part V of the Act.

This proposal makes sense, however it would involve a significant cultural change given the way freedom of information has evolved as a vehicle for obtaining access to personal files. Freedom of information is used to obtain files for litigation purposes. In this and possibly other instances the line between personal and non-personal information may become blurred, for instance in relation to evaluative or decision making records. This might necessitate making separate applications under each Act. The proposal could further restrict rights of access to personal information unless other proposals to require the Privacy Commissioner to make determinations and for these to be externally reviewed were also adopted.

This proposal also has implications for the proposed uniformity between Commonwealth, state and territory privacy laws so far as public sector information is concerned, where state privacy laws are subordinated to freedom of information laws and access to personal information is subject to FOI exemptions.

Question 12–1 What exceptions should apply to the general provision granting an individual the right to access his or her own personal information held by an agency?

For example, should the exceptions mirror the provisions in Part IV of the Freedom of Information Act 1982 (Cth) or should another set of exceptions apply?

The exemptions under freedom of information legislation are designed to protect the operation of government, and tend to apply imperfectly to the regulation of access to personal information, even though this has become the main function of such legislation. Without going into detail we would argue that the individual's interest in accessing his or her personal information should be

given a higher priority than access to other kinds of information and the barriers should be correspondingly reduced. To some extent this issue is already addressed by provisions such as section 36(1)(b) of the *Freedom of Information Act 1982*, that introduce a public interest test and section 38(2) which except applications for personal information. Such provisions could be extended with a clearer indication of how the public interest should be applied.

Required or authorised by or under law

Question 13–1 Should the definition of a 'law' for the purposes of determining when an act or practice is required or specifically authorised by or under a law include:

(a) a common law or equitable duty;

(b) an order of a court or tribunal;

(c) documents that are given the force of law by an Act of Parliament, such as industrial awards; and

(d) statutory instruments such as a Local Environmental Plan made under a planning law?

Question 13–2 Should a list be compiled of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the Privacy Act? If so, should the list have the force of law? Should it be comprehensive or indicative? What body should be responsible for compiling and updating the list?

Legal Aid Commissions frequently face demands to disclose information, in circumstances where we have to balance, privacy, confidentiality and client privilege against the powers that an authority claims to exercise.

We see value in providing more explicit statutory guidance on when information can be collected, use or disclosed in ways which would otherwise breach the Privacy Act. However we foresee problems in extending the definition of required or specifically authorized under law to common law and equitable duties, without further qualification. Such duties are inherently elastic and, if broadly applied, could significantly impact on the protection provided by privacy laws.

Financial transaction legislation (proposals 13-3 to 13-4)

The review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), the regulations and the Anti-Money Laundering and Counter-Terrorism Financing Rules under s 251 of the Act should consider, in particular, whether:

(a) reporting entities and designated agencies are appropriately handling personal information under the legislation;

(b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;

(c) it remains appropriate that reporting entities are required to retain information for seven years; and

(d) it is appropriate that reporting entities are able to use the electoral roll for the purpose of identification verification.

The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) should be amended to provide that state and territory agencies that access personal information provided to the Australian Transaction Reports and Analysis Centre under the Act be regulated under the Privacy Act in relation to the handling of that personal information, except where they are covered by obligations under a state or territory law that are, overall, at least the equivalent of all the relevant obligations in the Privacy Act.

We support both proposals. The scope of these powers and their potential impact on financial privacy is so wide; that the public should be assured that information should only be used for purposed defined by the legislation. The approach should be uniform across jurisdictions.

Notification (proposal 20-6)

The Office of the Privacy Commissioner should provide guidance on the circumstances in which it is necessary for an agency or organisation to notify an individual when it has received personal information about the individual from a source other than the individual concerned.

Organisations that rely on third party information provided by a client in order to provide a confidential service can be genuinely puzzled about how to notify third parties without compromising client confidentiality.

Legal Aid Commissions receive information about third parties, to assist in determining an individual's eligibility for legal aid, and in connection with providing legal assistance. The latter function is generally covered by client privilege. The former may require departures from current privacy legislation. We therefore see merit in this recommendation.

Privacy impact assessments

Proposal 27–5 Before the introduction by agencies of any unique multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should consider the need for a privacy impact assessment.

Proposal 44–4 The Privacy Act should be amended to empower the Privacy Commissioner to:

(a) direct an agency or organisation to provide to the Privacy Commissioner a privacy impact assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and

(b) report to the Minister an agency or organisation's failure to comply with such a direction.

Proposal 44–5 The Office of the Privacy Commissioner should develop Privacy Impact Assessment Guidelines tailored to the needs of organisations.

We support the proposal for a mandatory privacy impact assessment before Government agencies introduce unique multi-purpose identifiers.

While we support leaving the decisions about whether other new Government and organisational projects require a privacy impact assessment at the discretion of the Privacy Commissioner, we would like to see a mechanism whereby the Privacy Commissioner must consider representations from concerned organisations and people both when initiating an investigation on the need for a PIA and when determining whether to require one. Legal Aid Commissions and other non-government agencies that assist the more vulnerable members of the community have a valuable contribution to make on the adverse effects of the kind of new proposals the proposals seek to address.

Defence and intelligence information handling

Proposal 31-1 The privacy rules and guidelines, which relate to the handling of intelligence information concerning Australian persons by the Australian Security Intelligence Organisation, Australian Security Intelligence Service, Defence Imagery and Geospatial Organisation, Defence Intelligence Organisation, Defence Signals Directorate and Office of National Assessments, should be amended to include consistent rules and guidelines relating to:

(a) incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of the incident and measures taken to protect the privacy of the Australian person);

(b) the accuracy of personal information; and

(c) the storage and security of personal information.

Proposal 31–5 The privacy rules and guidelines referred to in Proposal 31–1 should be made available electronically to the public; for example, on the websites of those agencies.

We support the above proposals together with the other proposals relating to specific intelligence and oversight agencies. Australian citizens and residents

facing the exercise of extraordinary powers under anti-terrorist legislation need to have at least some basic assurance of the integrity of the information giving rise to investigation and charges.

Federal courts and tribunals

Proposal 32–1 Federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.

Question 32–1 Should the Privacy Act be amended to provide that federal tribunals are exempt from the operation of the Act in respect of their adjudicative functions? If so, what should be the scope of 'adjudicative functions'?

We support proposal 32-1 as a means of encouraging research into legal service delivery and promoting the accountability of the court system, while maintaining the general exclusion of the courts' non –administrative functions.

In relation to federal tribunals we see value in the proposal for a more limited exemption to cover adjudicative functions, though we would question whether this should take the form of a blanket exemption from the proposed uniform privacy principles or could be practically achieved by an appropriate exemption from those principles which do not fit with adjudicative functions.

Removing the small business exemption

Proposal 35-1 The Privacy Act should be amended to remove the small business exemption by:

(a) deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and

(b) repealing ss 6D–6EA of the Act.

Proposal 35-2 Before the proposed removal of the small business exemption from the Privacy Act comes into effect, the Office of the Privacy Commissioner should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by:

(a) establishing a national small business hotline to assist small businesses in complying with the Act;

(b) developing educational materials—including guidelines, information sheets, fact sheets and checklists—on the requirements under the Act;

(c) developing and publishing templates for small businesses to assist in preparing Privacy Policies, to be available electronically and in hard copy free of charge;

and

(d) liaising with other Australian Government agencies, state and territory authorities and representative industry bodies to conduct programs to promote an understanding and acceptance of the privacy principles.

We support the extension of the coverage of the Privacy Act to cover small businesses and other organisations. This would resolve uncertainties which currently prevent members of the public from exercising their privacy rights or identifying the obligations of organisations they deal. As we discuss elsewhere coverage of non-government organisations that provide funded public services would avoid some of the complications which arise in the way legal services are provided.

Uniform coverage means that organisations and individuals can rely on clearly stated privacy obligations when dealing with small businesses and non government organisations, and on forms of alternative dispute resolution under the Privacy Act as a realistic alternative to legal action. Uniform coverage should ease the task of the Privacy Commissioner when providing education and advice.

Removal of the small business exemption, ensuring that information remains relevant and giving the Privacy Commissioner the power to develop a binding code for a particular industry, there is no need for separate laws to regulate the way residential tenancy databases collect and give access to personal information. Most of the grievances that have arisen from the way these databases operate can be addressed by the application of normal privacy principles. However additional measures may be necessary to ensure renters can access their own information without unreasonable costs or delays that sometimes currently apply.

We agree there will be a need for extra assistance in helping small organisations to understand and meet their added compliance obligations.

Employee records exemption proposals 36-1 to 36-2

Proposal 36–1 The Privacy Act should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.

Proposal 36–2 The Privacy Act should be amended to provide that an agency or organisation may deny a request for access to evaluative material, disclosure of which would breach an obligation of confidence to the supplier of the information.

'Evaluative material' for these purposes means evaluative or opinion material compiled solely for the purpose of determining the suitability, eligibility, or qualifications of the individual concerned for employment, appointment or the award of a contract, scholarship, honour, or other benefit

We support the proposition that employees should have access to employee records beyond the limited access provided under the *Workplace Relations Act*. The definition of employee records for the purpose of the current exemption is too broad and means that employers can accumulate a considerable range of information about employees covering sensitive matters like health, drug tests and other disciplinary issues without being accountable for the way they handle it.

We have reservations about the scope of the proposed exemption for evaluative material, particularly insofar as it covers adverse employment references. The common law on liability for negligent references is still in a state of development. There is scope for a more robust debate on whether those who provide references should be able to rely on confidentiality where information is malicious or intended to prevent an employee from obtaining employment elsewhere.

Media Exemption

Proposal 38–1 The Privacy Act should be amended to define 'journalism' to mean the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

(a) material having the character of news, current affairs or a documentary; or

(b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary.

Proposal 38–2 In consultation with the Australian Communications and Media Authority and peak media representative bodies, the Office of the Privacy Commissioner should establish criteria for assessing the adequacy of media privacy standards for the purposes of the media exemption.

Proposal 38–3 The Office of the Privacy Commissioner should issue guidelines containing the criteria for assessing the adequacy of media privacy standards established under Proposal 38–2.

Proposal 38–4 Section 7B(4)(b)(i) of the Privacy Act should be amended to provide that the standards must 'deal adequately with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters)'.

We support moves for greater clarity of the scope of the media exemption under the Privacy Act. We have specific concerns about reporting details of

people involved in legal matters where this involves a breach of law, court orders or is a consequence of a breach of privacy by a law enforcement agency or other body. Some form of civil or administrative accountability would be preferable to the penal sanctions that apply to such actions.

One concern is the need for clear standards in relation to the responsible reporting of matters involving children. An important issue in our view is the affect that publication may have on the rehabilitation of children who have committed offences and on their families.

Private investigators

Question 40–1 Should the Australian Government request that the Standing Committee of Attorneys-General consider the regulation of private investigators and the impact of federal, state and territory privacy and related laws on the industry?

National regulation of the information gathering activities of private investigators lacks consistency and would benefit from a greater degree of uniformity. However we would not support a general exemption for investigators from privacy legislation as this would imply that their activities, which by their nature impose a pressure on personal privacy are subject to less accountability than over civilian occupations.

Alternative dispute resolution schemes

Question 40–2 Should the Privacy Act or other relevant legislation be amended to provide exemptions or exceptions applicable to the operation of alternative dispute resolution (ADR) schemes? Specifically, should the proposed:

(a) 'Specific Notification' principle exempt or except ADR bodies from the requirement to inform an individual about the fact of collection of personal information, including unsolicited personal information, where to do so would prejudice an obligation of privacy owed to a party to the dispute, or could cause safety concerns for another individual;

(b) 'Use and Disclosure' principle authorise the disclosure of personal and sensitive information to ADR bodies for the purpose of dispute resolution; and

(c) 'Sensitive Information' principle authorise the collection of sensitive information without consent by an ADR body where necessary for the purpose of dispute resolution?

We support the proposed limited exemptions for ADR schemes. The definition of an ADR scheme for this purpose requires further development given the wide variety of schemes, different degrees of organisation and the extent to

which some schemes also perform other functions which may involve the handling of personal information.

For example ADR under the *Family Law Act* may be undertaken by sole practitioners, employees of bodies providing other social assistance services or under the auspices of Legal Aid Commissions. Provisions of the *Family Law Act* and Regulations prescribe some aspects of the way they handle information as may the Acts that constitute Legal Aid Commissions. An ADR scheme established to comply with the Privacy Act or other legislation may have an entirely different focus and orientation.

Relationship between codes and unified privacy principles (proposal 44-9)

Part IIIAA of the Privacy Act should be amended to specify that:

(a) privacy codes approved under Part IIIAA operate in addition to the proposed UPPs and do not replace those principles; and

(b) a privacy code may provide guidance or standards on how any one or more of the proposed UPPs should be applied, or are to be complied with, by the organisations bound by the code, as long as such guidance or standards contain obligations that are at least equivalent to those under the Act.

The recommendation that codes should operate in addition to privacy principles and not replace them may not take sufficient account of the effect of other proposals including more uniform Commonwealth and state regulation, and elimination of existing exemptions. Codes represent a way in which organisations or sectors can comply with the spirit of the principles without being held to requirements that they cannot practicably comply with. For example Public Interest Determinations 9 and 9A override NPP 10.1 so as to permit health providers to collect health information about a patient's relatives. Legal Aid Commissions similarly need to access information about third parties to assess the means of an applicant for legal aid in circumstances where seeking third party consent to collection is similarly impracticable. Now may be an appropriate time to codify such provisions. However it seems inherently unlikely that all such exemptions can be anticipated through general provisions in the legislation.

Determination of complaints (proposals 45-6 and 45-7

Section 52 of the Privacy Act should be amended to empower the Privacy Commissioner to make an order in a determination that an agency or respondent must take specified action within a specified period for the purpose of ensuring compliance with the Act.

The Privacy Act should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner under s 52 and the current review rights set out in s 61 should be repealed.

We support the recommendation that the Privacy Commissioner be required to make a formal determination where complaints cannot be conciliated or dismissed for lack of response by the complainant.

We support giving the Privacy Commissioner the power to make enforceable orders and to apply to have these enforced through the Federal courts.

Data breach notification

Proposal 47–1 The Privacy Act should be amended to include a new Part on data breach notification, to provide as follows:

(a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

(b) An agency or organisation is not required to notify any affected individual where:

(i) the specified information was encrypted adequately;

(ii) the specified information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the proposed Unified Privacy

We support a requirement for organisations that have exposed customer or client information through a lapse in security. This should avoid unduly burdening small businesses and customers/clients who are informed of a breach. This could involve a two stage reporting process whereby an initial report is made to the Office of the Privacy Commissioner, which then determines if and whether customers or clients should be individually advised. Organisations should not be able to secure customer consent to a waiver of the obligation to notify or require customers to indemnify them against the effects of any notified breach.

Credit reporting

Legal Aid Queensland's submission includes more detailed comments on the credit reporting proposals. We confine ourselves to the following.

Proposal 50–1 The credit reporting provisions of the Privacy Act should be repealed and credit reporting regulated under the general provisions of the Privacy Act and proposed Unified Privacy Principles (UPPs).

Proposal 50–2 Privacy rules, which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information, should be promulgated in regulations under the Privacy Act—the proposed Privacy (Credit Reporting Information) Regulations.

Proposal 50–5 The proposed Privacy (Credit Reporting Information) Regulations should apply only to the handling by credit reporting agencies and credit providers of personal information maintained by credit reporting agencies and used by credit providers in assessing an individual's credit worthiness. This category of personal information should be defined as 'credit reporting information'.

We support the proposal to replace Part IIIA with coverage for credit providers and credit reporting agencies under the private sector provisions, but with a continuation of some special provisions in the regulations. Our submission can not address all the proposals in Parts 50 to 55. However some of them do appear to give rise to some complex interactions that would concern legal professions and organisations that assist disadvantaged clients with credit problems.

Proposal 50–6 The definition of a 'credit reporting business' in the proposed Privacy (Credit Reporting Information) Regulations, if based on that in s 6(1) of the Privacy Act, should exclude the phrase 'other than records in which the only personal information relating to individuals is publicly available information'.

We support this proposal. The expression "publicly available information" is too vague, given widespread availability of on-line databases. Data from some sources, such as those related to legal action should still be subject to privacy standards such as accuracy and relevance when compiled for credit assessment purposes.

Proposal 50–7 The proposed Privacy (Credit Reporting Information) Regulations should include a simplified definition of 'credit provider' under which those individuals or organisations who are currently credit providers for the purposes of Part IIIA of the Privacy Act (whether by operation of s 11B of the Privacy Act or pursuant to

determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.

We disagree with the effect of proposal 50-7 which would mean that a comparatively large number of organisations who provide consumer credit as an incidental part of their business activities will have access to the enlarged class of data proposed under Part 51 of the Discussion Paper. We do not consider that the principle of reciprocity in proposal 51-2 provides an adequate safeguard against the potential for this information to be used for purposes that are only indirectly related to the assessment of credit, for instance under proposal 53-2.

More comprehensive credit reporting (proposals 51-1 to 51-

Proposal 51–1 The proposed Privacy (Credit Reporting Information) Regulations should permit the inclusion in credit reporting files of the following categories of personal information in addition to those currently permitted under s 18E of the Privacy Act:

(a) the type of each current credit account opened (for example, mortgage, personal loan, credit card);

(b) the date on which each current credit account was opened;

(c) the limit of each current credit account (for example, initial advance, amount of credit approved, approved limit); and

(d) the date on which each credit account was closed.

Our concerns in relation to the proposed expansion of the contents of a credit report are related to the continuation or expansion of the organisations that have access to the main consumer credit reporting databases. The risk is too great that comprehensive information about individuals finances will be used for a range of purposes that go beyond simply assessing the creditworthiness of an applicant for credit. We are not convinced that the increase in information will mean that lenders will lend more responsibly. Experience overseas, particularly in the United States, is that whilst the percentage of defaults has dropped the number of defaults has increased substantially.

We have argued that an increase in the availability of information needs to be accompanied by legislation requiring all lenders to lend responsibly.

Collecting credit information

Proposal 52–1 The proposed Privacy (Credit Reporting Information) Regulations should provide for the recording, on the initiative of the relevant individual, of information that the individual has been the subject of identity theft.

We support this proposal. The industry has informed us that notations on files are never read by the credit provider nor inform their lending decisions. Veda is proposing that the customer have the option of "freezing" their report and only making the report available when they "unfreeze" it. We would support such a proposal subject top the following condition. Credit providers who do not access the credit report before assessing an application for credit should not be able to list a default, if the account has been frozen and they are unable to prove that the debt was incurred by the named debtor.

Proposal 52–2 Credit reporting agencies only should be permitted to list overdue payments of more than a minimum amount.

Question 52–1 Should the proposed Privacy (Credit Reporting Information) Regulations provide a minimum amount for overdue payments listed by credit reporting agencies? If not, by what mechanism should a minimum amount for overdue payments be set and enforced?

We strongly support a minimum amount for overdue payments to be listed. The minimum amount should be large enough to justify the expense of taking more substantial recovery action than a standard warning letter and not so small as too penalise people for inadvertently overlooking a utility payment. It should have the capacity to increase in line with inflation. While lacking empirical data to support a specific limit, some members of NLA consider the currently accepted limit of $100 fails this test and should be increased to $500, with built in consumer price index adjustments.

Proposal 52–3 The proposed Privacy (Credit Reporting Information) Regulations should not permit credit reporting information to include information about presented and dishonoured cheques, as currently permitted under s 18E(1)(b)(vii) of the Privacy Act.

We support the proposal.

Proposal 52–4 The proposed Privacy (Credit Reporting Information) Regulations should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index (NPII) administered under the Bankruptcy Regulations 1966 (Cth).

Proposal 52–5 Credit reporting agencies, in accordance with obligations to ensure the accuracy and completeness of credit reporting information, should ensure that credit reports adequately differentiate the forms of administration identified on the NPII.

We share the concerns expressed about listing debt agreements along with other insolvency information and would support the distinctions proposed in proposal 52-5.

Question 52–2 Should the proposed Privacy (Credit Reporting Information) Regulations allow for the listing of a 'serious credit infringement' or similar and, if so, how should this concept be defined?

We would restate our earlier concerns about the imprecise scope of clause (c) of the definition of serious credit infringement. We question the need to expand the scope of the definition beyond actual fraudulent conduct or conduct which gives rise to a reasonable suspicion of intention to defraud the credit provider.

Question 53–2 Should credit providers be permitted to use credit reporting information to 'pre-screen' credit offers? If so, should credit providers be required to allow individuals to opt out, or should credit providers only be permitted to engage in pre-screening if the individual in question has expressly opted in to receiving credit offers?

We are unable to give an unequivocal answer to this question. On the one hand pre-screening could assist in the responsible marketing of credit by reducing offers to vulnerable consumers. On the other hand pre-screening could reduce opportunities for the most disadvantaged people in the community. Broad definitions of consumer credit and credit provider mean that people with poor or incomplete credit histories are excluded from access to consumer services through a process they have very little control over. Pre screening could also be used to undermine the prohibition on direct marketing as lists could be "washed" to obtain certain sets of consumers. For example "consumers with housing loans", "consumers with housing loan defaults", "consumers with more than one credit card etc".

Proposal 54–3 The proposed Privacy (Credit Reporting Information) Regulations should provide that credit reporting agencies must:

(a) enter into agreements with credit providers that contain obligations to ensure data quality in the information credit providers provide to credit reporting agencies;

(b) establish and maintain controls to ensure that only information that is accurate, complete, up-to-date and relevant is used or disclosed;

(c) monitor data quality and audit compliance with the agreements and controls; and

(d) identify and investigate possible breaches of the agreements and controls.

We support the recommendation to give credit providers and credit reporting agencies responsibility to ensure the information they hold is accurate, complete, relevant and up to date.

Question 55–1 Should the proposed Privacy (Credit Reporting Information) Regulations provide that individuals have the right to obtain a free copy of their credit reporting information?

Yes. It is inequitable and inconsistent with privacy for credit reporting agents to force individuals with credit problems to pay for access to the information they need to access to resolve these problems, which other people provided about them.

Proposal 55–3 The proposed Privacy (Credit Reporting Information) Regulations should provide that the information to be given if an individual's application for credit is refused based wholly or partly on credit reporting information should include any credit score or ranking used by the credit provider, together with explanatory material on scoring systems, to allow individuals to understand how the risk of the credit application was assessed.

We support this proposal.

Proposal 55–4 The proposed Privacy (Credit Reporting Information) Regulations should provide that:

(a) credit reporting agencies and credit providers must handle credit reporting complaints in a fair, efficient and timely manner;

(b) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint;

(c) a credit reporting agency should refer to a credit provider for resolution of a complaint about the content of credit reporting information provided to the agency by that credit provider; and

(d) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint it must immediately inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

We consider the proposal should go further and require all entities having access to credit reporting to belong to an independent dispute process that meet ASIC's Regulatory Guide 139 and with the capacity to determine liability

for a debt at least for the purposes of establishing whether a debt was overdue.

Research

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

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

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

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

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

Proposal 58–8 The research exception to the proposed 'Collection' principle should state that, despite subclause 2.6, an agency or organisation may collect sensitive information about an individual where:

(a) the collection is necessary for research;

(b) the purpose cannot be served by the collection of information that does not identify the individual;

(c) it is impracticable for the agency or organisation to seek the individual's consent to the collection;

(d) a Human Research Ethics Committee has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the UPPs; and

(e) the information is collected in accordance with rules issued by the Privacy Commissioner.

Where an agency or organisation collects sensitive information about an individual in accordance with this provision, it must take reasonable steps to ensure that the

information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

Legal Aid Commissions have a particular interest in the proposal to broaden the kinds of research for which data can be disclosed subject to an ethics approval process. We hold significant amounts of information which is in demand for social and legal research. We believe that ethically informed and regulated research has an essential role to play in addressing issues of disadvantage, and promoting informed policy on criminal law enforcement. However it is important to reconcile the sometimes competing priorities of researchers and research subjects in a way that does not sacrifice one to the other or undermine the autonomy and dignity of the most disadvantaged groups (Chalmers & Israel 2005).

We support the recommendations in principle, but consider they should be qualified in some respects. There is a need to safeguard other interests of research subjects, for example those associated with legal professional privilege and the potential impact that research findings in relation to legal issues can have on small and identifiable populations.

There is a need to entrench the privacy rights of research subjects, so that they can not be too easily overridden by political priorities.

There is a need to address the burden placed on research ethics committees in having to determine privacy issues which are often of a technical legal rather than a specifically ethical nature. (Dodds & ors 2002) If research ethics committees are to continue to serve as the primary mechanism for approving research where it is impracticable to obtain subject consent, there should be greater accountability in the way decisions are reached. This would be assisted by better thought out and more detailed reporting requirements for ethics committees. Accountability could also take the form of affected people having the ability to seek Privacy Commissioner review of ethics determinations.

Children's capacity to consent

Proposal 60–1 The Privacy Act should be amended to provide that:

(a) an individual aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access unless found to be incapable (in accordance with the criteria set out in Proposal 60–2) of giving that consent, making that request or exercising that right;

(b) where it is practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, an assessment about the individual's capacity should be undertaken; and

(c) where it is not practicable to make an assessment about the capacity of an individual aged 14 or under to give consent, make a request or exercise a right of access, then the consent, request or exercising of the right to access must be provided by an authorised representative of the individual.

Proposal 60–2 The Privacy Act should be amended to provide that an individual aged under 18 is incapable of giving consent, making a request or exercising a right if, despite the provision of reasonable assistance by another person, he or she is incapable, by reason of maturity, injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability or any other circumstance, of:

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

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

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

We have reservations about fixing an arbitrary age of 15 below which children are presumed to lack the capacity to consent under privacy legislation. We would prefer a continuation of the practice whereby presumptions about the capacity of children to consent is dependent on their understanding and the implications of disclosing specific kinds of personal information

As Legal Aid Commissions we represent children in sensitive criminal and family law contexts where it is important to obtain instructions and other information from the children themselves and where the interests of children are not necessary identical with those of their legal guardians. Issues of consent involving children will often arise in highly sensitive situations where their solicitor needs to form a judgement about their capacity to instruct or provide information. In some situations practitioners' ability to obtain this information will be covered by exemptions under privacy legislation or by

overriding legal authorisation however there will be some situations where an arbitrary presumption will complicate access to information.

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

We support this proposal, particularly in relation to reporting about children involved with the legal system. Despite laws and professional ethical codes which are supposed to apply in this area, there are still significant lapses. The best guarantee that children's privacy is respected is a complementary approach that draws on different levels of regulation.

Adults with a temporary or permanent incapacity

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

Proposal 61-1 The Privacy Act should be amended to provide that an individual aged 18 or over is incapable of giving consent, making a request or exercising a right under the Act if, despite the provision of reasonable assistance by another person, he or she is incapable by reason of injury, disease, illness, cognitive impairment, physical impairment, mental disorder, any disability, or any other circumstance, of:

(a) understanding the general nature and effect of giving the consent, making the request or exercising the right; or

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

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

Proposal 61-2 The Privacy Act should be amended to introduce the concept of 'authorised representative', defined as a person who is, in relation to an individual:

(a) a guardian of the individual appointed under law;

(b) a guardian for the individual under an appointment of enduring guardianship;

(c) an attorney for the individual under an enduring power of attorney;

(d) a person who has parental responsibility for the individual if the individual is under the age of 18; or

(e) otherwise empowered under law to perform any functions or duties as agent or in the best interests of the individual.

The Privacy Act should state that an authorised representative is not to act on behalf of the individual in any way that is inconsistent with an order made by a court or

tribunal, in contravention of the terms of any appointment under law, or beyond the powers provided for in an enduring power of attorney.

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

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

(a) was not properly appointed; or

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

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

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

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

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

Agencies and organisations that regularly handle personal information about adults incapable of making a decision should ensure that there are trained adequately to assess the decision-making capacity of individuals.

We agree that there is a need to clarify consent requirements under privacy legislation for people with diminished capacity. Legal aid commissions frequently face situations where providing assistance to such clients is complicated by the lack of a clear framework outside the established frameworks of guardianship and the like. At the same time we agree that as far as possible the expressed wishes of people should be respected and carried out. We therefore would answer yes to questions 61-1 and 61-2. The guidance on how to assess capacity under proposal 61-4 would serve a useful purpose in this respect.

However we believe that the scope of authority proposed for an "authorised representative" is too restrictive and might mean that advocates who are assisting persons with an impaired capacity are unable to obtain the information even with the consent of the person. An authorised representative

should include someone authorised to act for the person either in writing or verbally for a limited or extended duration or purpose. Experience suggests that otherwise such requirements are used to restrict people with impaired capacity from accessing their own information.

Telecommunication interception issues

Proposal 63–1 The Australian Government should initiate a review to consider the extent to which the Telecommunications Act 1997 (Cth) and the Telecommunications (Interception and Access) Act 1979 (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how the Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation; and

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Australian Government Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance.

We support the proposed review of the two Acts to better integrate law enforcement access to intercept and traffic data to apply to all interception warrants. The review should also cover the use of telecommunications data by state and territory law enforcement agencies having regard to the lack of uniform coverage for state law enforcement agencies under privacy laws.

Question 63–2 Does the Telecommunications (Interception and Access) Amendment Bill 2007 provide adequate protection of personal information that is used or disclosed for law enforcement purposes? For example, should the Bill be amended to:

(a) define 'telecommunications data';

(b) provide greater guidance on how the privacy implications of an authorisation should be considered and documented under proposed s 180(5);

(c) include positive obligations on law enforcement agencies to destroy in a timely manner irrelevant material containing personal information and information which is no longer needed; and

(d) provide that the Inspector-General of Intelligence and Security monitor the use of powers by the Australian Security Intelligence Organisation to obtain prospective telecommunications data?

Proposal 64–1 Section 79 of the Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

Proposal 64–2 The Attorney-General's Department should provide guidance on when the chief officer of an agency must cause information or a record to be destroyed when it is no longer required for a permitted purpose under s 79 and s 150 of the Telecommunications (Interception and Access) Act 1979 (Cth). This guidance should include time limits within which agencies must review holdings of information and destroy information as required by the legislation.

Measures to provide clearer guidance and oversight on permissible interception would be supported. However recent cases under anti-terrorist legislation suggest the need for caution when imposing a requirement for the timely destruction of irrelevant and no longer required intercept material. Evidence of intercepted communications can be selectively presented. We do not consider that privacy should become a pretext for destroying material that might be required in order to view a communication in its proper context or to investigate a possible misuse of intercept material.

Question 64–3 Should further restrictions apply in relation to the use and disclosure of information obtained by a B-party interception warrant under the Telecommunications (Interception and Access) Act 1979 (Cth)?

Proposal 64–3 Section 79 of the Telecommunications (Interception and Access) Act 1979 (Cth) should be amended to expressly require the destruction of non-material content intercepted under a B-party warrant.

The power under section 46 to disclose information obtained from warrants to intercept a particular service used by people other than the target of an investigation for a variety of law enforcement and disciplinary functions goes beyond the legitimate law enforcement justification for intercepting private communications. Indefinite retention of such data for possible future uses is equally inconsistent with democratic values. Disclosure of non –relevant material obtained through B-party warrants should be limited to exceptional cases involving national security or a serious risk to life, health or property. Non-material content should be quarantined and eventually destroyed.

Question 64-4 Should the regime relating to access to stored communications under the Telecommunications (Interception and Access) Act 1979 (Cth) be amended to provide further reporting requirements in relation to the use and effectiveness of stored communications warrants?

Access to stored communications should be subject to the same restrictions as access to voice intercepts. The current distinction relies on the argument that text based communications are more considered than spoken communications and that therefore people should be more accountable and less protected for what they commit to text. In reality the choice of communication method reflects factors such as age, income, access and cultural orientation so that the distinction is a discriminatory one that creates risk of selective surveillance of particular groups.

Proposal 64–4 The Office of the Privacy Commissioner should be made a member of the Australian Communications and Media Authority's Law Enforcement Advisory Committee.

We support this proposal, having regard to the significant expansion of interception powers to cover stored messages.

Conclusion

Thank you for the opportunity to provide this submission and for the extension of time in which to lodge it. If you have any questions please do not hesitate to contact John Gaudin on (02) 9219 5695 or via e-mail: john.gaudin@legalaid.nsw.gov.au.

Yours sincerely,

Hamish Gilmore
Chairperson
National Legal Aid

Works referred to

Chalmers R & Israel M (2005) *Caring for data, law, professional codes and the negotiation of confidentiality in Australian criminological research*, Report Commissioned by AIC

Dodds S, McNeil Paul, Chalmers, D & ors (2002) Special issue on future of Human Research Ethics Committees: *Monash Bioethics Law Review* 21, 3, 43

Read C (2007) *Taking Sides on Technology Neutrality* 4:3 SCRIPT-ed 263