Executive Summary

Contents

Introduction to the ALRC's Privacy Inquiry 103
Extensive public engagement 105
The scope of the *Privacy Act* 106
The National Privacy Phone-In 107
The general lamentation: is privacy passé? 107
An emerging generation gap? 108
Complexity and confusion 109
Enforcing compliance 109
The BOTPA excuse: 'Because of the *Privacy Act*' 109
Key recommendations 110
The *Privacy Act* and privacy principles 110
National consistency 112
Key definitions 112
Rationalisation and clarification of exemptions 113
Improved complaint handling 116
Stronger penalties 117
The structure and role of the OPC 117
Data breach notification 117
Decision making by children and young people 118
Nominee arrangements 119
More comprehensive credit reporting 120
Privacy and telecommunications 122
Health information 122
Greater facilitation of research 123
Cross-Border data flows 124
Statutory cause of action for a serious invasion of privacy 126
Further reviews and studies 128

Introduction to the ALRC's Privacy Inquiry

For Your Information: Australian Privacy Law and Practice represents the culmination of a 28 month inquiry into the extent to which the *Privacy Act 1988* (Cth) and related laws continue to provide an effective framework for the protection of privacy in Australia. This Inquiry was a mammoth undertaking, resulting in the three volumes of this Report, containing 74 chapters and 295 recommendations for reform.

The *Privacy Act* is itself substantially the product of an earlier ALRC inquiry—a seven year research and policy development exercise ending in 1983 with the publication of the three volume report entitled *Privacy*.[1] As discussed in Chapter 1, the enactment of privacy legislation in Australia represented partial fulfilment of Australia's international obligations under the *International Covenant on Civil and Political Rights*, which recognises a basic human right to privacy premised on the autonomy and dignity of the individual.[2] The ALRC's work not only led to domestic legislation but also strongly influenced the international development of this field. The ALRC's Chair at that time, Justice Michael Kirby, was asked to chair two key Organisation for Economic Co-operation and Development working groups in the 1980s, on privacy principles and data security.

As a recognised human right, privacy protection generally should take precedence over a range of other countervailing interests, such as cost and convenience. It is often the case, however, that privacy rights will clash with a range of other individual rights and collective interests, such as freedom of expression and national security. Although the ALRC often heard emphatic arguments couched in the language of rights, international instruments on human rights, and the growing international and domestic jurisprudence in this field, all recognise that privacy protection is not an absolute. Where circumstances require, the vindication of individual rights must be balanced carefully against other competing rights—and the ALRC's final recommendations in this Report endeavour to do so.

The privacy implications of developing technology were not lost on the Commission in 1983—and the ALRC was surprisingly prescient in its understanding of emerging computer power and the associated privacy concerns. However, the now ubiquitous use of personal computers, mobile phones and cameras, the internet, radio frequency identification devices, global positioning systems, surveillance cameras, smart cards, biometrics and a myriad of other technological developments—while perhaps not quite in the realm of science fiction in the 1980s—was yet to impact so comprehensively and powerfully on the daily lives of Australians.

In the new Information Age, high-powered computers and other sophisticated electronic devices are no longer the preserve of specialist technicians employed by governments and major corporations, but a basic tool utilised by virtually all Australians in almost all aspects of their lives, including for: communication with family, friends and colleagues; research and writing; entertainment and news gathering; shopping, banking and share trading; storage of important records, documents and images; and dating and social networking.

---

1 Australian Law Reform Commission, *Privacy*, ALRC 22 (1983).

2 *International Covenant on Civil and Political Rights*, 16 December 1966, [1980] ATS 23, (entered into force generally on 23 March 1976), art 17.

It became clear during the course of the current Inquiry that these rapid advances in information, communication and surveillance technologies have created a range of previously unforeseen privacy issues. At the same time, the emergence of regional political and economic blocs, such as the European Union and the Asia-Pacific Economic Cooperation group (APEC), has created pressure for the alignment of Australia's privacy protection regime with those of its key trading partners.

Further, information privacy legislation has proliferated at the state and territory level, but with no concerted effort to maintain a nationally consistent regime. Finally, the *Privacy Act* has undergone significant amendment since its enactment in 1988, resulting in an unwieldy and overly complex piece of legislation.

Extensive public engagement

The breadth of the subject matter covered in this Inquiry required the ALRC to undertake the largest community consultation program in its 33 year history. To facilitate public engagement and stakeholder participation, two issues papers, *Review of Privacy* (IP 31)[3] and *Review of Privacy: Credit Reporting Provisions* (IP 32),[4] and a three-volume Discussion Paper, *Review of Australian Privacy Law* (DP 72),[5] were released. Concise overviews of IP 31 and IP 32,[6] and DP 72,[7] also were published to reach the non-specialist audience. The ALRC organised:

- about 250 face-to-face meetings with individuals, organisations and agencies;
- major public forums in Melbourne (focusing on consumers and privacy), Sydney (focusing on business and privacy) and Coffs Harbour (focusing on health privacy and research);
- six workshops for children and young people (aimed at those aged 13–25);
- a series of roundtables with individuals, agencies and organisations on a variety of themes including: credit reporting; telecommunications; the privacy principles; children and young people; and health and research;

3 Australian Law Reform Commission, *Review of Privacy*, IP 31 (2006).
4 Australian Law Reform Commission, *Review of Privacy—Credit Reporting Provisions*, IP 32 (2006).
5 Australian Law Reform Commission, *Review of Australian Privacy Law*, DP 72 (2007).
6 Australian Law Reform Commission, *Reviewing Australia's Privacy Laws: Is Privacy Passé?*, Overview (2006).
7 Australian Law Reform Commission, *Review of Australian Privacy Law: An Overview of Discussion Paper 72* (2007).

- a highly publicised 'National Privacy Phone-In' on 1–2 June 2006, during which more than 1,300 members of the public contacted the ALRC to share their experiences, ideas and attitudes about privacy protection (see below); and

- the establishment of a 'Talking Privacy' website, designed specifically to appeal to young people.

The ALRC also actively solicited submissions, receiving 585 written submissions from a broad cross-section of individuals, organisations and agencies. The high level of public engagement with the ALRC Inquiry reflected the extent of public interest and concern about privacy protection. Community and stakeholder concerns helped direct the ALRC in developing its priorities and the ultimate reform agenda.

The scope of the *Privacy Act*

In the early stages, at least, some meetings suggested that there was a mismatch in the broader concept of privacy utilised by the general public and the way the term 'privacy' is defined in a technical legal sense in the *Privacy Act*. Experts and privacy professionals mainly concern themselves with information privacy and data security and protection. The ALRC has, in fact, recommended that the name of the Act be changed to the *Privacy and Personal Information Act*.[8]

Australians generally consider that they have a 'right to privacy'—notwithstanding the absence of a national charter of rights—and that this protection has been extended to cover the activities of the private sector as well as government agencies. Many members of the general public (and no doubt many lawyers), however, incorrectly assume that the *Privacy Act* also covers such others matters as:

- unwanted calls at home by telemarketers (now addressed by the 'Do Not Call Register');

- surveillance at work and in public places;

- spying by neighbours;

- paparazzi-type photographs; and

- police procedures, especially intrusive searches and seizures and the collection of DNA samples.

8 See Ch 5.

The National Privacy Phone-In

The ALRC kicked off the public phase of the Inquiry with a two day National Privacy Phone-In on 1–2 June 2006, which handled 1,343 responses. The results were very interesting. Nearly three-quarters of all respondents (73%) cited telemarketing as a major concern, provoking a cluster bomb of indignant questions and comments: 'It feels like a "home invasion"'; 'How did they get my number?'; 'Why do they always call at dinner time when I've got my hands full cooking and trying to settle the kids?'

This category was followed, in order of prevalence, by concerns expressed about:

- the handling of personal information by the private sector (19%);
- the handling of personal information by government (9%);
- the protection of privacy on the internet (7%);
- national identity cards and 'smart cards' (7%);
- problems accessing and correcting personal information (7%); and
- surveillance in public places (4%).

Contrary to expectations, very few comments were received about workplace surveillance (2%) or spying by neighbours (only four calls).[9]

The general lamentation: is privacy passé?

It was very evident in public forums and meetings that there is a general feeling in the community that technological advances have steadily and irreparably eroded personal privacy—'we have much less privacy than previous generations, and it will only get worse!'—and that greater efforts must be made to resist this.

When the discussion moved from the general to the specific, however, there was evident a countervailing appreciation of the parallel benefits of modern information and communication technology, with praise for the ease, convenience and empowering qualities of email, mobile phones, e-commerce, digital photography, the internet and so on.

---

9 Callers were able to nominate more than one concern, which is reflected in the statistics. Further, the nature of the comments may have been influenced by a number of media stories about the Phone-In, which focused on telemarketing as a possible concern.

People also expressed a high degree of willingness to trade off privacy interests (or at least to understand the potential compromise) to meet concerns about law and order at the local level—for example, accepting the use of surveillance cameras in public places—or about national security more generally.

Similarly, the ALRC found—despite the frequent use of the absolutist language of 'rights'—that there is general community appreciation for the need to strike a common sense balance between privacy interests and practical concerns in a range of areas. For example, while personal health information is regarded as 'sensitive' and deserving of the highest level of protections, individuals understand that a premium may be placed on prompt access to, and disclosure of, such information in the case of a medical emergency.

An emerging generation gap?

During the course of this Inquiry, the ALRC explored whether there is an emerging generation gap in basic attitudes to privacy. That is, do young people have such a fundamentally different approach to privacy that this should be recognised (or at least anticipated) by law?

It does appear that young people are more comfortable than their parents, and certainly their grandparents, in sharing personal information, photos and other material on social networking websites. The question is whether this represents the beginnings of an enduring cultural shift, or simply the eternal recklessness of youth, played out in a new medium and utilising new technology. Put another way, will today's teenagers be horrified in a decade's time when prospective employers—and prospective partners and in-laws—can easily 'google up' intimate and potentially embarrassing images and information?

As mentioned above, the ALRC went to considerable effort to consult directly with children and young people—and found that, even though there is an increased willingness to share information on websites like MySpace and Facebook, nevertheless there remains a strong desire to retain control over access to, and distribution of, this personal information. Some young people were quite savvy about how to achieve this. Many others, however, appeared to be unaware of the privacy policies of the social networking sites they frequented, and unfortunately naïve about the degree of control they can exercise in practice. Further, many young people were unaware of the extent to which information—for example, photographs—deleted from their profile remain on the internet; either as a result of downloading onto other sites or archiving.

While children and young people normally can seek guidance about moral and ethical standards of behaviour at home, at school or at their place of worship, they may find themselves pretty much on their own when operating at the cutting edge of technology.

The ALRC found, however, that there was little appetite for more law or formal regulation in this area. The consistent advice received was that much more education is

needed for children and young people—and the adults in their lives—about how to operate properly and safely in this new electronic environment. Some excellent guidance already is being published by industry bodies, and the ALRC recommends that this effort intensify and also involve the Office of the Privacy Commissioner (OPC).

Complexity and confusion

Businesses—not surprisingly—were concerned mainly with the overly complex and confusing web of privacy laws in Australia, citing the overlapping federal, state and territory laws; the separate privacy principles for government agencies (the Information Privacy Principles (IPPs)) and private sector organisations (the National Privacy Principles (NPPs)), and other relevant laws, including those covering the privacy of health information. This makes it very difficult—and expensive—for even the best-intentioned business to comply.

These concerns were expressed consistently and strongly in submissions and consultations throughout the Inquiry—making it clear to the ALRC that simplification and harmonisation of the law had to be one of the principal aims and outcomes of this Inquiry.

Enforcing compliance

The ALRC often heard concerns that the *Privacy Act* is a 'toothless tiger', lacking adequate enforcement mechanisms and sufficient sanctions to ensure compliance. Whether this is a real or a perceived problem, the ALRC takes very seriously the need to improve the regulatory scheme and to increase community confidence in the level of compliance with the requirements of the Act.

The ALRC actively sought and received community and stakeholder comment in this area, and makes a number of recommendations (see below) aimed at addressing: the structure, role and powers of the OPC; improvements to the complaint-handling process; the Privacy Commissioner's ability to require a Privacy Impact Assessment for a new project or development that may have a significant impact on the handling of personal information; the Privacy Commissioner's powers to conduct audits, monitor compliance, and to issue notices to comply where required; greater powers for the OPC to spur the development of context or industry-specific privacy codes, to flesh out the general privacy principles; and the ability of the OPC to pursue civil penalties in a federal court, where there is a serious or repeated misuse of an individual's personal information.

The BOTPA excuse: 'Because of the *Privacy Act*'

Interestingly, a range of callers to the National Privacy Phone-In argued that sometimes there may be '*too much* privacy'—or rather that 'privacy' is all too often trotted out as an excuse for inaction or non-cooperation. Among privacy professionals,

this has become known as the 'BOTPA' excuse, since people are told that their reasonable requests cannot be accommodated 'because of the *Privacy Act*'. For example, the ALRC heard complaints from people who, 'because of the *Privacy Act*', were unable to:

- access or correct their own personal information held on a government or corporate database;
- assist an elderly relative or neighbour with their banking, or in dealing with a public utility or government agency—even where that person had written authorisation or held a valid power of attorney; and
- urge their church congregation to pray for a named individual who was unwell and in hospital.

Key recommendations

Having listened carefully to the views, concerns and feedback expressed during the extensive community consultation exercise, and conducted its own research and deliberations, the ALRC has developed and presents in this Report a large set of policy recommendations for improving privacy protection in Australia. Some of the key recommendations are explained below.

The *Privacy Act* and privacy principles

The ALRC recommends that the *Privacy Act* be redrafted and restructured to achieve significantly greater consistency, clarity and simplicity.

A key element of this reform would be a rationalisation of the privacy principles, which address the handling of personal information by agencies and organisations covered by the *Privacy Act*. There are currently two separate sets of privacy principles contained in the *Privacy Act*:

- the IPPs, which apply to the handling of personal information by Commonwealth and ACT public sector agencies; and
- the NPPs, which apply to many private sector organisations (including not-for-profit organisations, but not most small businesses).

The ALRC recommends that these be unified into a single set of privacy principles, covering information handling in both the public and private sectors. For the purposes of this Inquiry, these principles are referred to as the model Unified Privacy Principles (UPPs),[10] and cover the following areas:

---

10 The ALRC anticipates that the principles may be renamed when the *Privacy Act* is redrafted.

- Anonymity and Pseudonymity;
- Collection;
- Notification;
- Openness;
- Use and Disclosure;
- Direct Marketing;
- Data Quality;
- Data Security;
- Access and Correction;
- Identifiers; and
- Cross-Border Data Flows.

The ALRC sees 'principles-based regulation' as the primary method of regulating information privacy in Australia. It is important to note, however, that the ALRC does not recommend the adoption of a pure form of principles-based regulation. In order to achieve the necessary policy outcomes, the ALRC adopts a pragmatic approach to the formulation of the model UPPs and its recommended regulatory model. For example, in some circumstances, the UPPs will need to be supplemented with more specific rules (promulgated in regulations or other legislative instruments), in order to accommodate the particular needs and circumstances of different industries.

The ALRC recommends a basic restructure of privacy regulation to follow this three-tiered approach:

- high-level principles of general application, provided in a streamlined *Privacy Act*;
- regulations and industry codes, detailing the handling of personal information in certain specified contexts, such as health and research, and credit reporting; and
- guidance issued by the Privacy Commissioner (and other relevant regulators), dealing with operational matters and explaining to end users what is expected in various circumstances, as well as providing basic advice and education.

National consistency

The Australian Government is not alone in seeking to regulate the handling of personal information in Australia—every state and territory also has legislation or administrative guidelines in this area. This creates confusion for individual consumers, who cannot always be expected to know whether an agency is a federal, state or territory body or, as a result, where to go for guidance on which privacy laws apply or where to take concerns and complaints.

In addition to general information privacy legislation, New South Wales, Victoria and the ACT also have specific laws on the handling of health information, which apply to state public sector agencies and private sector organisations. This creates uncertainty for health service providers and consumers, because private health services (including not-for-profit health services) may be covered by the federal *Privacy Act*, as well as by specific state or territory health privacy legislation. Health services that operate across state and territory borders may have to comply with multiple laws, each with different requirements.

There is little doubt that there would be great benefits across the board from adopting a common approach to privacy protection in all Australian jurisdictions. To achieve greater consistency, the ALRC recommends that the *Privacy Act* should apply to the federal public sector and the private sector—to the exclusion of state and territory laws dealing specifically with the privacy of personal information, including personal health information, handled by organisations.

The Commonwealth, state and territory governments should establish an intergovernmental cooperative scheme, under which the states and territories will agree to enact legislation to regulate the handling of personal information in each state's and territory's public sector by adopting the key elements of the *Privacy Act*—such as the same set of privacy principles, important definitions, data breach notification schemes and other key provisions.

The approach recommended by the ALRC would make it far easier for individuals to understand the general rules that apply to personal information—regardless of whether it is being handled by a private organisation, a federal agency, or a state or territory agency—and would ease the compliance burden significantly and reduce costs for business.

Key definitions

Important definitions in the *Privacy Act*—such as the definition of 'personal information', 'sensitive information' and 'record'—should be updated to deal with new technologies and new methods of collecting and storing personal information.

The definition of 'personal information' should be amended to bring it more into line with other jurisdictions and international instruments.

Sensitive information—which is given a higher level of protection than other personal information under the NPPs—is defined in the *Privacy Act* to include information about particular types of personal characteristics, including racial or ethnic origins, political opinions, religious beliefs and sexual orientation. The ALRC heard concerns that biometric technologies—such as facial and gait recognition systems—may be used without an individual's knowledge or consent, and could reveal other sensitive personal information, such as information about a person's health or racial or ethnic origins. To address this concern, the ALRC recommends that the definition of 'sensitive information' be amended to include certain types of biometric information.

The definition of 'record' should be amended to ensure greater consistency with other legislation, and to clarify that a record may be stored in electronic or other formats.

Rationalisation and clarification of exemptions

The current fragmentation and complexity of privacy protection in Australia is exacerbated by the number of exemptions from, and exceptions to, the requirements of the *Privacy Act*. Complete exemptions from the coverage of the Act should be permitted only where there is a compelling policy basis for so doing. The ALRC recommends that the number of exemptions be reduced—in particular, the existing exemptions for small business, employee records and registered political parties should be removed.

The small business exemption

When the provisions of the *Privacy Act* were extended to cover the private sector in December 2000, an exemption was granted to small businesses (including not-for-profit organisations) with an annual turnover of $3 million or less.[11] The exemption was explained, at that time, by the desire to achieve widespread acceptance for privacy regulation from the private sector, and a reluctance to impose additional compliance burdens on small businesses.

No other comparable jurisdiction in the world exempts small businesses from the general privacy law—and the European Union specifically has cited this unusual exemption as a major obstacle to Australia being granted 'adequacy' status under the European Union *Directive on the Protection of Individuals with Regard to the*

11 There are some exceptions to this general rule—for example, small health service providers handling sensitive personal information.

Processing of Personal Data and on the Free Movement of Such Data (the EU Directive).[12]

The business community argued strongly for the retention of the exemption, primarily on the basis of the cost of compliance. However, almost all other stakeholders supported removal of the exemption arguing that there is no compelling justification for a blanket exemption for small businesses, as consumers have the right to expect that their personal information will be treated in accordance with the privacy principles.

The ALRC recommends that this exemption be removed. This would bring Australian privacy laws into line with laws in similar jurisdictions, such as the United Kingdom (UK), Canada and New Zealand, and could facilitate trade by helping to ensure that Australia's privacy laws are recognised as 'adequate' by the European Union. The removal of the small business exemption would have the additional benefits of simplifying the law and removing uncertainty for many small businesses that have difficulty establishing whether they are required to comply with the *Privacy Act*.

The ALRC appreciates that the removal of the small business exemption will have cost implications for the sector—although nowhere near as great as is sometimes predicted.[13] An independent research study commissioned by the ALRC indicated that a lower proportion of organisations will be affected—since not all small businesses collect personal information from customers—and the costs should be considerably more modest—about $225 in start-up costs and $301 per year thereafter for each small business—than the predicted $842 and $924 per year respectively cited in the Office of Small Business costing.[14] Further, the ALRC is confident that additional savings will be achieved by the substantial simplification and harmonisation of privacy laws recommended in this Report.

Nevertheless, the ALRC remains attentive to the economic concerns of small business owners, and recommends a number of other initiatives aimed at supporting small businesses and minimising the compliance burden. Before the exemption is removed, the OPC should provide support to small businesses to assist them in understanding and fulfilling their obligations under the *Privacy Act*. This should include a national hotline for small businesses, education materials and templates to assist in preparing privacy policies.

---

12 European Parliament, *Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, Directive 95/46/EC (1995).

13 See Australian Government Office of Small Business, *Costing into the Review of the Privacy Act 1988* (2007), as discussed in Ch 39.

14 Ibid.

Employee records exemption

While public sector agencies are required to treat employee records in accordance with the *Privacy Act*, private organisations generally are exempt in relation to current and past employees (with some limited exceptions). There seems little justification in principle for the differential approach—which does not feature in the law of comparable jurisdictions.

The ALRC recommends that this exemption be removed. This would create consistent rules for personal information about employees, regardless of whether they are public or private sector employees.

The ALRC acknowledges that there may be circumstances in which it is undesirable to allow employees to have access to all of the information contained in their files—such as referees' reports and other similarly confidential material. It would be much better practice to deal with such exceptions on the basis of the general law of confidentiality, however, rather than wholly exempting private sector employers from the normal requirements of the *Privacy Act*.

The 'Access and Correction' principle in the model UPPs permits an organisation or agency to deny a request for access to personal information in certain circumstances. For example, where access by an employee to evaluative material, such as references, would lead to a breach of confidence by the organisation, the organisation would be able to deny access on the basis that it is required or authorised by or under law.

Political parties, acts and practices exemption

Registered political parties are specifically excluded from the definition of 'organisation' and, therefore, are exempt from the operation of *Privacy Act*. In addition, political acts and practices of certain organisations—including political representatives, volunteers for political parties, and contractors and subcontractors of political parties and political representatives—are exempt from the Act.

In Australia, as in other western countries, the major political parties compile sophisticated databases containing a great deal of information about the contact details, concerns and preferences of individual voters. This assists the parties in election planning, fundraising, and developing policies and advertising strategies. Arguments supporting the exemption generally are based on the importance of freedom of political communication to Australia's robust democratic process. The position varies in other comparable countries—political parties are similarly exempt in the United States (US) and Canada, but compliance with privacy laws is required in the UK, New Zealand and Hong Kong.

There was considerable support in the general community, however, for removing the exemption. Some stakeholders argued that the preferential treatment accorded

registered political parties undermines public trust in the political process. Others were concerned that because of the exemption: political parties can collect information about constituents from third parties that could be inaccurate; individuals do not know what information has been collected by the parties; and have no right of access to, or correction of, personal information in electoral databases.

Journalism exemption

The acts and practices of a media organisation in the course of journalism are exempt from the operation of the *Privacy Act* where the organisation has publicly committed to observe standards that deal with privacy. This exemption reflects the balancing of competing rights, discussed above, placing a premium on protecting freedom of expression and the importance of the free flow of information to the maintenance of a healthy democracy.

No serious case was presented for the abolition of this exemption. There were some calls for refining the terms used to define it because of the difficulties associated with distinguishing journalism from commercial and other activities (especially in the convergent electronic environment).

The ALRC recommends that the scope of this exemption be clarified, by inserting a definition of 'journalism'—not currently defined in the Act. The ALRC also recommends that for the exemption to apply to an organisation, the standards to which the organisation is committed must *adequately* deal with privacy.

Improved complaint handling

The ALRC recommends the streamlining of procedures for handling complaints about alleged privacy breaches. The Privacy Commissioner should have the power to decline to investigate a complaint if, for example, the complaint is being handled by an appropriate external dispute resolution scheme.[15] Further, both complainants and respondents should have the power to require that the complaint be resolved by determination if, in the opinion of the Privacy Commissioner, all reasonable attempts to settle the complaint have failed.

Where the Privacy Commissioner determines that an agency or organisation has engaged in conduct constituting an interference with the privacy of an individual, the Commissioner should have the power to issue a notice prescribing that an agency or organisation must take specified action within a specified period, for the purpose of ensuring compliance with the *Privacy Act*. The Privacy Commissioner also should

15 The term 'external dispute resolution' (EDR) is used in this Report to refer to the resolution of complaints or disputes by an entity (other than a court, tribunal or government regulator) that is external to the organisation subject to the complaint or dispute. The term includes, but is not limited to, EDR conducted by EDR schemes approved by the Australian Securities and Investments Commission: see *Corporations Act 2001* (Cth) ss 912A(2)(b), 1017G(2)(b).

have the power to commence proceedings in the Federal Court of Australia or the Federal Magistrates Court for an order enforcing the notice.

Stronger penalties

There are currently no civil penalties available for serious contraventions of the Act, and only limited (and rarely used) criminal penalties for credit reporting and tax file number offences. The ALRC recommends that the penalty regime be strengthened by allowing the Privacy Commissioner to seek a civil penalty in the federal courts where there is a serious or repeated interference with the privacy of an individual.

The structure and role of the OPC

The ALRC recommends that the OPC be renamed the Australian Privacy Commission. The *Privacy Act* also should be amended to provide for the appointment of one or more Deputy Privacy Commissioners, with the power to exercise all the powers, duties and functions of the Privacy Commissioner. This would allow the agency to expand in response to technological developments and evolving public interest in privacy. It also would allow for greater collegiate decision making, encouraging greater accountability and transparency.

Further, the *Privacy Act* should be amended to increase the powers of the Privacy Commissioner, to include the power to:

- direct an agency to provide a 'Privacy Impact Assessment' in relation to a new project or development that may have a significant impact on the handling of personal information; and

- conduct 'Privacy Performance Assessments' of the records of personal information maintained by organisations.

Data breach notification

Under existing law, agencies and organisations are not required by the IPPs or NPPs to notify individuals when their personal information has been compromised. The ALRC's attention was directed to the strong growth internationally of requirements to notify individuals where there has been unauthorised access to their personal information. For example, about 40 American states now have data breach notification schemes, contained in legislation or administrative arrangements.

It was suggested in many meetings and submissions that a data breach notification scheme was needed in Australia, with a strong preference for a national approach overseen by the OPC. People are now very aware of the nefarious activities of computer hackers and the widespread existence of 'malware', and there are regular news reports of laptops containing sensitive personal information being lost and other personal records accidentally being exposed or illicitly accessed. Particularly given the

increasing fear of identity theft and fraud, proponents argue that individuals have a right to be informed when the security and privacy of their personal information have been compromised.

In terms of regulatory theory, there are good justifications for a national data breach notification scheme, including that:

- under-reporting of breaches is highly likely, absent any express requirement;
- this would provide strong market incentives to secure databases in compliance with the 'Data Security' principle;
- this would promote greater transparency and accountability around information-handling practices;
- notification gives individuals the information and opportunity to protect themselves against fraud and identity theft; and
- the development of a national model is preferable to a proliferation of differing state and territory schemes—as has happened in the US.

On the other side, the ALRC heard concerns from agencies and organisations about: the costs associated with notification, particularly where the relative risk of harm to individuals is small; the dangers of 'notification fatigue'; and a desire not to scare people away from e-commerce and other online services.

While recognising the sense and inevitability of some form of data breach notification scheme in Australia, agencies and organisations argued for one that adopted a reasonable balance, triggered only where there is a real risk of significant harm to individuals, and without unduly prescriptive or costly mechanics of notification (in terms of form, content, timing and method of distribution).

The ALRC recommends that the *Privacy Act* be amended to require an agency or organisation to notify the Privacy Commissioner and affected individuals when a data breach has occurred that may give rise to serious harm to any affected individual.

Decision making by children and young people

Issues relating to the privacy of children and young people often were raised in meetings and submissions. There is evident uncertainty in the community about the extent to which young people have the capacity to make decisions for themselves about the collection, use and disclosure of their personal information.

The *Privacy Act* is currently silent about the age at which children and young people should be able to make decisions about their own personal information.

Although arising in a range of circumstances, the biggest concern raised in consultations related to the use and disclosure of health and medical information—for example, whether young people (under the age of 18) could ask their family doctor not to disclose their personal health information to parents; and conversely whether parents could seek access to their teenage children's health records. (Note that consent to medical treatment—as opposed to the collection, use and disclosure of health information—is *not* a matter regulated by the *Privacy Act* and therefore is not considered in this Report).

Research on child development and adolescent brain development suggests that the capacity to make decisions evolves through childhood and adolescence, and is dependent on individual characteristics and the particular decision concerned. As in other inquiries in which similar issues have arisen—including the ALRC's reports on the rights of the child[16] and uniform evidence laws[17]—the ALRC has sought to shift the debate away from the imposition of a fixed age for decision making, towards an assessment (where possible) of the young person's capacity to make decisions about personal information.

For this reason, the ALRC has not recommended that the *Privacy Act* set a fixed age at which children and young people are deemed to be able to make their own decisions. Instead, the ALRC recommends that where it is practicable to make an assessment about capacity, such an assessment should be undertaken.

The ALRC recognises, however, that there are some situations in which it is difficult for an agency or organisation to make an assessment about decision-making capacity. The ALRC recommends that, where such an assessment is not reasonable and practicable, an individual aged 15 years or over should be presumed to be capable of giving consent, making a request or exercising a right of access concerning his or her personal information. This is consistent with the age at which a young person is able to obtain a separate Medicare card without parental consent. Individuals under the age of 15 must have a person with parental responsibility make the decision on their behalf, where it is not possible to assess decision-making capacity.

Nominee arrangements

The ALRC also heard many stories from people who were frustrated in their efforts to assist adult relatives and friends who are unable to act for themselves due to some temporary or permanent incapacity. It appears that in many of these cases the problems were occasioned by an incorrect or inflexible application of the *Privacy Act*. Similarly, some individuals may have the capacity to make their own decisions about privacy, but

16 Australian Law Reform Commission, *Seen and Heard: Priority for Children in the Legal Process* (ALRC 84, 1997).

17 Australian Law Reform Commission, *Uniform Evidence Laws* (ALRC 102, 2005).

need assistance in dealing with agencies or organisations—for example, due to limited mobility or language difficulties.

The ALRC makes a number of recommendations in this Report aimed at clarifying the legal position, to facilitate authorised persons rendering assistance in such cases—and minimising the 'BOTPA' problem. First, the *Privacy Act* should be amended to include the concept of a 'nominee', appointed by an individual, to make decisions and requests in relation to the individual's personal information. Once established, the agency or organisation should deal with an individual's nominee, to the extent provided in the nominee arrangement, as if the nominee were the individual concerned.

Further, the ALRC recommends that the OPC publish guidance for agencies and organisations on the proper involvement of third parties in communicating and making privacy decisions for those requiring assistance.

More comprehensive credit reporting

Little comment was aroused from the general public about the issue of credit reporting—but there was a very high level of engagement with the Inquiry in this area from credit providers and credit reporting organisations on the one hand, and privacy advocates and consumer groups on the other.

Perhaps unbeknown to most members of the community, Part IIIA of the *Privacy Act* regulates the system of credit reporting, allowing information about an individual's credit worthiness to be collected and disclosed to credit providers, such as banks, finance companies, mortgage companies, and mobile phone service providers. This information is collected by a small number of specialist credit reporting companies from credit providers and publicly available records.

The Australian regime is currently considerably more restrictive than in most comparable countries in relation to the types of information that may be collected and disclosed. Put simply, credit files are limited to information that might detract from an individual's credit worthiness, or so-called 'negative information'.

Credit providers and credit reporting bodies argued strongly for a wider range of information—such as current credit balances and loan repayment histories—to be collected and disclosed in reports to lenders, on the basis that such information is required for credit providers to make good decisions about an applicant's ability to service the requested level of debt. The industry was very active in supplying the ALRC with studies, surveys, reports and economic modelling suggesting that an increase in the 'positive' information available to lenders would facilitate better risk management practices, which in turn would open up the field to greater competition and drive down the cost of credit—especially for low risk and responsible borrowers.

At the same time, privacy and consumer advocates (and the Privacy Commissioner) argued strongly that allowing large amounts of sensitive information on the financial position and credit behaviour of individuals to be collected in private databases would pose greater risks to security and privacy—and, indeed, a number of previous inquiries into this area in Australia have failed to recommend any significant changes to the system.

The Australian credit industry itself is divided about how much more personal information is required—or, perhaps, is realistically obtainable given the opposition. Some credit providers pushed for 'comprehensive credit reporting' in keeping with practice in the US and the UK. During the life of the Inquiry, however, a consensus seemed to form around a more moderate approach—a system of 'more comprehensive credit reporting' that would add some additional categories of 'positive' information to an individual's credit information file, without going as far as the US or UK systems.

The ALRC recommends that the credit reporting provisions of the *Privacy Act* (Part IIIA) be repealed and credit reporting regulated under the general provisions of the Act (including the new credit reporting regulations), and the model UPPs.

Further, there should be some expansion of the categories of personal information that can be included in credit reporting information held by credit reporting agencies ('more comprehensive credit reporting'), to include: the type of each current credit account opened (eg, mortgage, credit card, personal loan); the date on which each current credit account was opened; the credit limit of each current account; and the date on which each credit account was closed.

The ALRC recognises that there are strong arguments in favour of also including an individual's repayment history in the categories of personal information that may be held by credit reporting agencies. The most compelling argument in favour of inclusion is that this will encourage more responsible lending practices. Some have questioned, however, whether more responsible lending will result from this change, in the absence of new obligations on credit providers.[18]

Consequently, the ALRC recommends that the Australian Government only amend the *Privacy Act* to allow credit reporting to include information about an individual's repayment history after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

---

18 That good risk management and responsible lending practices are not inevitable outcomes of comprehensive credit reporting is borne out by the major 'sub-prime loan' crisis in the US and the UK—where lenders have access to comprehensive information about prospective borrowers, but nevertheless made conspicuously poor decisions for years, based on the pursuit of market share and short-term incentives.

The ALRC's other recommendations for reform of credit reporting requirements include that credit providers should be prohibited from using or disclosing credit reporting information for the purposes of direct marketing, and may list overdue payment information only where the credit provider is a member of an external dispute resolution scheme approved by the Privacy Commissioner.

Privacy and telecommunications

While telecommunications legislation provides for unlisted or silent telephone numbers, it does not prohibit the charging of a fee to an individual who requests that his or her number not be listed in a public directory. The charging of a fee limits the ability of individuals—particularly those on low incomes—to control the use and disclosure of their personal information. The ALRC recommends that the charging of a fee for an unlisted (silent) number on a public number directory be prohibited by law.

A number of stakeholders told the ALRC that Part 13 of the *Telecommunications Act 1997* (Cth)—which deals with the use and disclosure of personal information in the telecommunications industry—is confusing and could be improved. The ALRC recommends that this Part of the *Telecommunications Act* be redrafted to achieve greater logical consistency, simplicity and clarity.

Health information

Overlap and complexity

There is a strong view in the community—reflected in the *Privacy Act*—that personal health information is 'sensitive information', requiring a high level of protection. A very significant concern in this area is the complexity, fragmentation and inconsistency of legislation and regulation relating to health privacy. As mentioned above, complexity is a serious concern across the whole field of privacy protection, but is perhaps most compelling in the regulation of health information.

Apart from the general recommendations made to promote national consistency,[19] the ALRC recommends that new *Privacy (Health Information) Regulations* be drafted, containing those requirements that are different or more specific than provided for in the model UPPs. Further, an intergovernmental agreement should be developed to ensure that the privacy regulation of health information (including relevant definitions) is harmonised across all Australian jurisdictions.[20]

Access to personal health information

The ALRC also heard many people express frustration about difficulties experienced in accessing or controlling their own health information—for example, patients who wished to have their medical records transferred to another doctor, whether for reasons of convenience or dissatisfaction with the services provided. Similarly, the ALRC

19 See Ch 3.
20 See Ch 3.

heard that there was a particular problem in gaining access to files where a health service closed (eg, where the doctor retired or passed away) or was taken over by another provider. The ALRC recommends that, in these circumstances, patients should be contacted and informed of the proposed arrangements for the transfer or storage of their medical records.[21]

Electronic health records

The Inquiry coincided with a number of major initiatives to develop an electronic record-keeping schemes by doctors and hospitals, aimed at providing better quality and safer health care—including the creation of a national shared electronic health information system, in which a summary of personal information is stored on a central database that can be accessed by a range of health service providers. For example, under this scheme, where an individual normally resident in New South Wales falls seriously ill or is involved in an accident in Queensland and is unable to communicate, local health authorities would be able to determine quickly whether the person suffered from any chronic medical conditions or allergies, and what medicines he or she had been prescribed.

Although there was widespread recognition of the obvious benefits of such a scheme, concerns were expressed about the architecture, security and privacy safeguards built into the system. The ALRC recommends that if national Unique Healthcare Identifiers or a national Shared Electronic Health Records scheme go forward, they should be established under specific enabling legislation, which addresses the key information privacy issues, including: the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems; the eligibility criteria, rights and requirements for participation in such schemes by health consumers and health service providers, including consent requirements; permitted and prohibited uses and linkages of the personal information held in the systems; safeguards in relation to the use of UHIs; and sanctions for misuse.[22]

Greater facilitation of research

The *Privacy Act* allows researchers to obtain and use personal information for health or medical research, without the consent of the individuals concerned, where approved by a Human Research Ethics Committee.

The ALRC heard many concerns, however, from researchers in the health and medical field—as well as social scientists, criminologists and others—that an overly cautious approach to the application of the *Privacy Act* was inhibiting the conduct of research, even where the threat to individual privacy was limited or non-existent and the

21 See Ch 63.
22 See Ch 61.

potential value of the research was very high. For example, epidemiological research can play a very valuable role in planning and promoting public health campaigns and in allocating scarce resources. In such cases, researchers are not concerned with the identity or information of individuals within the sample, but rather are seeking to identify broad trends and patterns in the population.

The ALRC also recognises that there are other forms of research that provide benefits to the community that require access to personal information in situations where it is difficult to obtain consent—such as research on child protection or factors associated with criminal behaviour.

The ALRC recommends that the research exception to the 'Collection' and 'Use and Disclosure' principles in the model UPPs allow information to be collected, used and disclosed for research purposes—including in areas other than health and medical research—where a number of conditions are met, including approval by a Human Research Ethics Committee.[23]

Cross-Border data flows

The ALRC quickly learned that an effective regulatory strategy cannot be developed under an outdated paradigm that assumes information can be contained within local or national borders, or that cross-border data flows are exceptional. It is now commonplace for major companies in Australia dealing with great volumes of personal information—including banks, insurance companies, credit card companies and others—to conduct their 'back office' processing of data overseas (often in Asia).

Indeed, privacy experts suggest it may be anachronistic even to talk about data 'flowing'—as if it there is a series of distinct, point-to-point transfers, when in fact this information is distributed across a number of databases and data centres in a number of countries, and is accessible globally by electronic means.

Similarly, individuals increasingly purchase goods and services over the internet on sites based overseas, paying with a credit card. A seemingly simple purchase of a book or DVD from a popular website, such as Amazon.com, actually may involve personal information flowing across many jurisdictions, with identity and credit verification, data processing, stock checking and shipping all handled in different countries.

Although now far more common than in previous decades, the concept of cross-border data flows is not something new. In Australia, the *Privacy Act* already deals with this phenomenon in NPP 9, which is modelled on arts 25–26 of the EU Directive.

---

23 See Chs 65, 66.

In both the ALRC's previous work on genetic privacy and discrimination (2001–2003)[24] and the current Privacy Inquiry, the ALRC consistently heard serious concerns expressed by members of the general public about their personal information being sent or held overseas without their express consent. In most cases, this unease did not reflect a specific critique of the adequacy or otherwise of the relevant privacy regime overseas—people simply do not know the position. Rather, it appears that this is a visceral reaction and an existential anxiety—a general feeling by people that they are losing control over something deeply personal, with little ability to do anything about it, and few remedies if things go badly wrong overseas.

For their part, however, business organisations told the ALRC they want to continue to be able to choose the most effective and efficient means of storing and processing customer data—and often this means doing so overseas. Indeed, businesses wish to develop these practices further, without the time, trouble and cost of seeking customer consent to what they regard as routine cross-border data flows. For business—and for governments promoting the economic benefits of efficient information handling and increasing access to global markets for trade and labour—the premium is on providing a framework to facilitate cross-border data flows, while providing individuals with a level of assurance that this will not compromise the security or privacy of their personal information.

During the course of this Inquiry, the Australian Government played a leading role in promoting the establishment of an effective regional privacy protection regime through its work with the APEC group. As evidenced by the ALRC's participation in meetings, the APEC Privacy Framework is an important opportunity to develop a distinctive approach in our region; one that is neither as reliant upon the private sector as the American regime, nor as heavily dominated by the bureaucracy as the European regime.

APEC can and should carve out a happy medium in this area, recognising the critical role that governments must play in regulating markets, but having due regard to ease and cost of compliance for business. While easy enough to articulate, developing a common approach will be no easy matter in practice, given the diversity among APEC members in cultural, political and economic terms. Achieving total uniformity, however, is not a precondition to cooperation—ultimately what is needed is a regime that Australia and other members can be sure will deliver high standards, consistency and accountability.

---

24 Australian Law Reform Commission and Australian Health Ethics Committee, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003).

While NPP 9 provides some protection for personal information transferred to another country by an organisation, it does not apply to government agencies; and a number of stakeholders suggested that it does not provide an adequate level of protection.

The ALRC recommends that the model UPPs include a 'Cross-Border Data Flows' principle. Under this principle an agency or organisation that transfers personal information about an individual outside Australia would remain accountable for that information, unless:

- the agency or organisation reasonably believes that the recipient or the information is subject to a law, binding scheme or contract that effectively protects the personal information in a manner that is substantially similar to the UPPs;

- the individual consents to the transfer, after being advised that the agency or organisation will no longer be accountable for personal information transferred if consent is provided; or

- the agency or organisation is required or authorised by or under law to transfer the personal information.

Statutory cause of action for a serious invasion of privacy

Jurisdictions in the US and Canada have legislated for a tort of invasion of privacy since the 1970s. While the courts in the UK do not recognise a tort by that name, the equitable action for breach of confidence has been used in practice to address the misuse of personal information, and the New Zealand courts also have recognised the existence of a common law tort of privacy.

In Australia, no jurisdiction has enshrined in legislation a cause of action for invasion of privacy. The door to the development of such an action at common law, however, was left open in 2001 by the High Court's decision in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*.[25] Since that time, lower court decisions in Queensland (2003) and Victoria (2007) have held that such a cause of action does indeed form part of the common law of Australia.

There was spirited debate during the Inquiry about the merits of legislating in Australia for a statutory cause of action for invasion of privacy. It is fair to say that media proprietors and most organisations are implacably opposed to the development of this cause of action—arguing that it would hinder investigative journalism and potentially infringe freedom of expression. Generally left unsaid is that photos and stories about the private lives of celebrities amount to big business, and poor practice would leave media organisations exposed to liability for damages.

---

25 *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

There was strong support for the development of a cause of action in the rest of the community, including among human rights and public interest organisations that generally are among the strongest advocates for freedom of speech—indicating again that this is an area requiring a careful balancing of important competing interests, rather than a blunt assertion of the rights of one sector. There is little doubt that advances in information and communication technology have heightened concerns about the potential for serious invasions of an individual's right to privacy.

Although the activities of assertive 'paparazzi' photographers feature in any conversation, most of the concerns expressed to the ALRC related more to the private sphere than to the mainstream media—and related to ordinary citizens rather than celebrities. For example, the ALRC heard stories of (or fears about) photographic images captured in toilets or dressing rooms via small digital cameras or phones, and then shown to others or posted on internet sites. There also were concerns about poor security and privacy practices—whether negligent or malicious—exposing sensitive personal information, such as medical or financial records, to unauthorised persons.

While the ALRC considers elsewhere (see above) a number of strategies for improving compliance—and penalising non-compliance—with the requirements of the *Privacy Act*, these do not provide a remedy directly to those individuals who have been harmed in the process. Further, the *Privacy Act* deals only with information privacy.

The ALRC was moved by the calls for the creation of a statutory cause of action for cases involving a serious invasion of privacy. Recognising the need to accommodate legitimate journalistic and artistic activities and uphold the right to freedom of expression, the bar must be set high and the cause of action limited to egregious circumstances.[26]

The ALRC recommends that federal legislation provide for a statutory cause of action for a serious invasion of privacy, in circumstances including where:

- there has been an interference with an individual's home or family life;
- an individual has been subjected to unauthorised surveillance;
- an individual's correspondence or private communication has been interfered with; or
- sensitive facts about an individual's private life have been disclosed.

26 See Ch 74.

The cause of action should apply only where the individual had a reasonable expectation of privacy; and the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

In addition, the court would be required to consider whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest in informing the public about matters of public concern and the interest in allowing freedom of expression).

Courts should be empowered to offer a range of tailored remedies for such breaches, including the award of aggravated (but not exemplary) damages, as well as injunctions, declarations and orders for apologies and corrections.

Examples of the sort of matters intended to fall within the ALRC's recommended statutory cause of action for serious invasion of privacy include the following:

- After the break-up of their relationship, Mr A sends copies of a DVD of himself and his former girlfriend (B) engaged in sexual activity to Ms B's parents, friends, neighbours and employer;

- Mr C sets up a tiny hidden camera in the women's toilet at his workplace, capturing images of his colleagues that he downloads to his own computer and transmits to a website hosted overseas, which features similar images; and

- Ms D works in a hospital and obtains access to the medical records of a famous sportsman, who is being treated for drug addiction. D makes a copy of the file and sells it to a newspaper, which publishes the information in a front page story.

Further reviews and studies

Given the breadth of this Report, and the far-reaching impact of a number of the recommendations, it will take some time to ascertain the effect of the recommended reforms. Consequently, the ALRC also recommends that the Australian Government initiate a review in five years from the commencement of:

- the amended *Privacy Act*, to consider whether the intergovernmental cooperative scheme recommended in this Report has been effective in achieving national consistency. If the review concludes that national consistency has not been achieved, the Australian Parliament should consider whether it should exercise its legislative power to cover the field, including in the state and territory public sectors; and

- the new *Privacy (Credit Reporting Information) Regulations*, to assess whether the policy objectives underpinning the regulations are being achieved.

In addition, some matters were considered by the ALRC to be outside the scope of this Inquiry. When considered appropriate, the ALRC has recommended a further inquiry or study. Examples include the recommendations that the Australian Government:

- undertake an inquiry to consider whether appropriate legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take;[27]

- fund a longitudinal study of the attitudes of Australians, in particular young people, to privacy;[28] and

- initiate a review to consider whether 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.[29]

27 See Ch 7.
28 See Ch 67.
29 See Ch 71.