BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 8, Number 9 September 2008

Commentary

News

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., U.S.A.

Legislation and Guidance

Review of Australia's privacy laws – grist for privacy globally

By Christine Cowper, Principal Consultant at Information Integrity Solutions Pty Ltd (ISS). IIS is a specialist privacy consultancy; its services include privacy impact assessments, privacy thought leadership and advice and strategy. Information about IIS is available at www.iispartners.com Chris can be contacted at: ccowper@iispartners.com

Introduction

Australian businesses and Government agencies are now waiting to see how Australia's federal Government will respond to the 295 recommendations in the Australian Law Reform Commission's (ALRC) report on its review of Australian Privacy Law.[1]

The Government sought the ALRC review in response to issues that have emerged in the eight years since the *Privacy Act 1988* (the Privacy Act) was extended to the private sector in 2000 and in the face of the huge changes in technology since the Act was introduced over twenty years ago. Although specific to the Australian context, the ALRC report explores issues that will be familiar to policy makers and organisations worldwide that are grappling with protecting individual privacy while supporting vibrant business innovation and effective government administration.

The ALRC conducted an extensive review over a two year period and has produced a detailed and wide-ranging report. While it does suggest a new statutory right of privacy, in general the report suggests a "host of refinements" rather than radical changes.[2] Its recommendations are intended to strengthen privacy protection for individuals, ease compliance obligations for business and government agencies and deal with some quite specific issues including the Australian approach to credit reporting.

With some notable exceptions, the public response to the report's recommendations has been generally accepting. This is probably in part due to the ALRC's extensive consultations and because the recommendations had been exposed, and in some cases negotiated, in the earlier phases of its inquiry.

As the Government considers the report, individuals, privacy advocates, business and government organisations will be asking which of the proposed refinements go far enough or too far and if they will be worth the change-over costs; business expects these to be considerable. An equally important question will be how robust the review is to future developments in technology, business models and global trade in personal information.

Background

The ALRC inquiry was initiated, amongst other reasons, because of the huge changes in technology since the Privacy Act was introduced in 1988. These change can be brought into focus by considering the almost unimaginable amount of personal information now being created and moreover the rate of change. For example, one report notes that:

> In 2006 161 exabytes (161 billion gigabytes) of digital information was created and copied, continuing an unprecedented period of information growth. This digital universe equals approximately three million times the information in all the books ever written. According to IDC, the amount of information created and copied in 2010 will surge more than sixfold to 988 exabytes, representing a compound annual growth rate of 57 per cent. The last time research of this type was attempted was in 2003 by researchers at the University of California, Berkeley, who came up with an information total of around five exabytes.[3]

It is not only the amount of personal information now circulating that is having an impact. The Internet, powerful computers and other technologies have sparked many new business models. More organisations are involved and both business and government organisations are using personal information in new ways; for example data analytics is now expanding from its traditional marketing base to other areas of the economy including fraud and identity, health and business metrics.[4]

Australia's privacy framework

Australia has a complicated array of privacy laws, in part because it has a federal system of government and aspects of privacy are regulated at federal and state and territory levels.[5] The laws generally draw on the international approaches for example in the Organisation for Economic Co-operation and Development (OECD) guidelines for the protection of privacy and transborder flows of information.

The federal Privacy Act, which is the key focus of the ALRC review, has expanded over time from its initial focus on federal public sector agencies, responding to factors such as:

- public concern about government proposals to introduce an identity card and to undertake extensive data-matching;
- public concern over the credit industry's intention to introduce a system of positive credit reporting; and
- business calls for measures to promote individual confidence in the information economy, and international developments including the European Union Data Protection Directive.

The resulting framework has several sets of privacy principles, including the Information Privacy Principles

(IPPs) which regulate public sector agencies, the National Privacy Principles (NPPs) which regulate the private sector and specific provision for the credit reporting industry. The Act also established the role of Privacy Commissioner with a range of powers and gave individuals a right to complain about an interference with their privacy.[6] [7] Initially the Privacy Act applied only to the federal public sector but was fairly quickly extended to the credit reporting sector, following. [8]

The private sector provisions were tailored to the business environment and recognised some strong business concerns by controversially exempting both small business and employee records from its coverage. The provisions are intended to be "light touch" and "co-regulatory". These approaches are reflected, for example, in that:

- the law is principled based rather than prescriptive;
- the Privacy Commissioner's monitoring and audit powers do not apply to organisations general information handling practices;
- there are limited options for enforcement or sanctions; and
- organisations can opt for a level of co-regulation, via an approved privacy code which must be at least as stringent as the NPPs.[9]

The ALRC process

In 2006, following reviews of the Privacy Act by the Privacy Commissioner and a Parliamentary committee that identified significant issues, the federal Government asked the ALRC to consider if the Privacy Act and related laws "continue to provide an effective framework for the protection of privacy in Australia".[10] [11] Issues for consideration included:

- the current privacy regulatory framework including federal, state and territory laws and practices;
- the impact of rapid advances in information, communication, storage, surveillance and other relevant technologies;
- developments in privacy trends and regulations in other jurisdictions;
- community views about privacy; and
- the regulatory burden on business.

The ALRC's final report and recommendations follow a very wide consultation process based on extensive legal research, detailed issues papers, and a discussion paper in which it exposed its possible recommendations. It has taken particular care to hear the views of groups that are often excluded from this sort of process and, for example, held focus groups and designed a website so that it could hear from young people. Over the course of its inquiry the ALRC held over 250 meetings and received 585 submissions from stakeholders including individuals, public sector agencies, private organisations, community groups and peak associations. The consultation process has been impressive and the final report can certainly claim that it is reflecting community opinion.

Report process including Government response

The ALRC presented its report to Government at the end of May and as is required by law the report was tabled in Parliament on 11 August 2008.[12] The Australian Government will now consider the ALRC's 295 recommendations and has said that it will do this in stages. The first stage of the response will focus on the recommendations relating to refinements to privacy principles, health and credit reporting regulations and improving education about the impact on privacy by new technologies should be delivered in twelve to eighteen months.[13] A timeframe for the response to other recommendations, including the controversial recommendation for a statutory private cause of action has not been announced. The ALRC report is only one input to the Government's policy process. It is open to the Government to adopt all, some or none of the ALRC's recommendations and ultimately it up to the Australian Parliament to consider any proposed changes to the legal framework.

Key ALRC recommendations

The ALRC report divides its discussion and recommendations into ten themes. The discussion under each theme is rich, drawing as it does on the ALRC's research and legal analysis as well as the consultation noted above.

Some of the key themes are set out briefly here.[14] The points noted are not intended to be a comprehensive summary.[15] Rather, the aim is to give an idea of the areas of inquiry, some of the views and some of the ALRC's key recommendations. The recommendations mentioned are of interest to the writers as they go to aspects of the Privacy Act which have most impact on the privacy of individuals and business operations. A feature of the ALRC's approach that is worth bearing in mind is that its recommendations often include, in fact in over 70 places, a role for the Privacy Commissioner to provide guidance material to assist agencies and businesses in applying the privacy principles or complying with the Privacy Act.

Developing technology

The ALRC report gives a thoughtful discussion of the impact on privacy of rapid advances in information, communication, storage, surveillance and other relevant technologies. Interestingly, while recognising that the application of new technologies raises very significant privacy issues the report does not recommend major changes to the Privacy Act or its principles. While some privacy advocates were skeptical that general principles would be robust in the face of unknown future technology developments, the ALRC found generally strong support for continuing the current "technology neutral" approach that sets high level privacy objectives rather than attempting to set rules to regulate a particular technology.[16]

However, the ALRC does recommend some refinements to the Privacy Act and principles to clarify its application to new technologies, for example:

- the definition of personal information is amended to recognise that a number of non-identified elements

combined, for example ISP or email address, can make an individual "reasonably identifiable"; and

- expand the notice requirements so that individuals are told how, when and from where information about them has been collected, thus exposing amongst other things the technology used to collect personal information.

It also recognises that the Privacy Act, even with such refinements, is not a full answer to the issues identified. It also notes the critical importance of a range of supporting strategies including:

- the use of privacy impact assessments and market forces;
- international engagement and co-operation; and
- individual empowerment, including through education and awareness and the use of privacy enhancing technologies.

The ALRC's recommendations provide a useful updating of the existing framework. However there is starting to be a view, reflected for example in projects recently initiated by the United Kingdom Information Commissioner and in work undertaken in Australia for the Privacy & Trust Partnership that the current frameworks need rethinking in the face of the radical changes that are taking place.[17]

The Privacy Principles

As noted earlier, the Privacy Act currently contains two main sets of privacy principles, the IPPs and the NPPs, as well as other rules including for the handling of credit reporting and tax file number information; the resulting framework is complex to understand and apply, adding to compliance costs and difficulty for individuals in being aware of and exercising their privacy rights.

As a consequence, the ALRC found very high levels of support for its proposed recommendations for the development of a combined set of principles, applying to both the public and private sectors, and which the ALRC called the Unified Privacy Principles (UPPs). While there was some concern about whether a single standard for agencies and organisations would work the value in terms of simplicity, transparency and cost effectiveness were well recognised.

The ALRC also undertook a very detailed, effectively line-by-line examination of the content of the two key sets of principles in terms of the intended objectives, on the ground experience and future challenges. This part of the discussion elicited vigorous and varying views.

Some of the key issues for debate included:

- the need for a definition of consent;
- the matters about which individuals should be advised when specific information is collected and about information handling practices generally;
- the rules for direct marketing;
- making reasonable provision for people with diminished decision-making capacity; and
- the protection of information transferred overseas.

The final report continues to attract a reasonable degree of support from consumer and privacy advocates; the changes in the transborder principle in particular have been welcomed.[18] The business community's focus at present is more on the cost of implementing the changes, which they expect to be considerable.

Overall the recommendations tend towards some tightening of the protections for individuals, particularly in relation to direct marketing, notice and transborder data flows, which now emphasise that agencies and organisations should be accountable for data transferred unless alternative protections are in place. However, while providing a very detailed and thorough review of the issues, effectively the ALRC's recommendations amount to incremental changes to existing privacy principles as set out for example in the OECD privacy guidelines and now articulated in many sets of privacy principles around the world.[19]

In the context of this inquiry this may have been as far as was possible to go. However, there is some thinking that suggests, for example, that the current reliance on notice and consent to promote individual control is struggling in the face of the volume of personal information circulating and how business are using/managing information.[20] This is perhaps a question for the next generation of privacy principles.

Exemptions

This part of the report considered the current exemptions and partial exemptions to the Privacy Act. The exemptions respond to a range of complex and legitimate interests including, for example, the protection of national security, the government's intention to limit regulatory costs for small businesses, general business concerns about regulatory obligations in relation their employees, the separation of powers in Australia's constitution, and the political process.

While recognising the importance of these interests, the ALRC concluded that exemptions only should be permitted where there is a compelling reason. It proceeded to recommend the removal of the exemptions for small business, employee records, political parties and political acts and practices.

The discussion of the various exemptions was again vigorous. In relation to employee records and small business, the ALRC considered matters such as:

- the recognition of the sensitivity of employee information and the limited protection currently found in workplace relations legislation;
- the fact that other jurisdictions, for example New Zealand and the United Kingdom, do protect employee records;
- the effect the exemptions have on the perception of Australia's law internationally, for example in relation to its failure to be assessed as 'adequate' under the European Union Directive; and
- for small business, the difficulty and complexity in exempting some small businesses and not others.

Some of the countervailing arguments included the impact on:

- management and the employment relationship, for example if required to disclose otherwise confidential and sensitive information;
- outsourcing arrangements or sale of a business; and
- regulatory burden and compliance costs.

The ALRC was not swayed by these arguments as it considered that many of the concerns raised could in fact be accommodated within the framework of the UPPs or in some cases were overstated.

There is strong support for these recommendations from many stakeholders, in particular privacy and consumer advocates. Arguably they provide for a more level playing field, reduce the overall complexity of the law and are likely to promote confidence in the strength of the privacy protection offered. However, the history of these exemptions and the reaction since the ALRC's report was released suggests that these recommendations may struggle to be implemented. For example, the Australian Chamber of Commerce and Industry call on the Government "not to proceed with the . . .recommendations which would impose far-reaching privacy law compliance and red tape costs on 1.8 million Australian small and medium businesses.[21]

The Government is not planning to respond to this set of recommendations as an early priority, and it will be an area to watch in the future.

Office of the Privacy Commissioner

The Privacy Act provides for a regulator, the Privacy Commissioner, and sets out the Commissioner's role and powers.[22]

The effectiveness of any regulatory framework depends on both the nature of the law and on how it is enforced.[23] In the past, the Act has been criticised by privacy advocates and others as being too "light touch" in this area. While the ALRC states that it is aiming for compliance rather than a punishment approach, its recommendations here amount to a significant strengthening of the Commissioner's powers and while also increasing accountability, via a new appeal process, to organisations and individuals. In particular, its recommendations include that the Privacy Commissioner:

- can be asked to make a formal determination in relation to a complaint and that such decisions can be subject to a merits review by the Administrative Appeals Tribunal;
- can, in formally determining a complaint, prescribe the steps that an agency or respondent must take to ensure compliance with the Act;
- seek a civil penalty in the Federal Court or Federal Magistrates Court where there is a serious or repeated interference with the privacy of an individual; and
- accept an undertaking that an agency or organisation will take specified action to ensure compliance with a requirement of the Privacy Act and to seek enforcement through the courts if such an undertaking is breached.

Overall these changes could be quite significant. They have the potential to give individuals greater confidence in the system, and to raise the profile of privacy within organisations; after an initial strong business response when the Privacy Act was extended in 2000 the issue has fallen back on the agenda for many organisations. Consumer and privacy advocates have cautiously welcomed this set of recommendations and in particular have supported the strengthened role for the Privacy Commissioner.

However, the resources available to the Commissioner will be a key factor in whether these measures, if implemented, are effective. This is particularly relevant given the high dependence throughout the ALRC report on guidance from the Privacy Commissioner's Office which is clearly likely to be a resource intensive activity.

The ALRC has also responded to international regulatory trends and is recommending that the Privacy Act provide for data breach notification. It proposes that government agencies and business organisations should be required to notify individuals—and the Privacy Commissioner—where there is a real risk of serious harm occurring as a result of a data breach. Interestingly, the ALRC amended its first proposals to set quite a high bar before notification is required.

Business might have been expected to be wary about the data breach provisions, particularly as Australia has not suffered the sort of major security breaches that triggered the introduction of data breach laws in the United States. However, the Government's announcement that this issue will be a second phase issue may have taken the heat out of the response.

Credit reporting provisions

The current Australian credit reporting rules are quite specific and prescriptive and carry heavy penalties for misuse of the system or credit reporting information. Unlike credit reporting in some other jurisdictions, here reporting is limited to "negative" reporting, that is very basic facts about individuals, limited reporting about loans applied for and negative events such as late repayment etc. It is also strictly limited to credit and does not cover other forms of reporting such as employment record or retail tenancy history.

The ALRC makes recommendations on two levels. Firstly, it seeks to simplify the regime by limiting specific credit reporting rules to matters not addressed in the UPPs; there is currently significant overlap. Secondly, it recommends that in addition to the limited types of "negative" information currently permitted, some additional categories of "positive" information should be allowed to be added to an individual's credit file, in order to facilitate better risk management practices by credit suppliers and lenders. The ALRC does seek legislation requiring "responsible lending practices" as a condition of some of the proposed changes.

The changes to the credit reporting provisions are very significant; they change the emphasis of the system from default reporting to more of a risk management. The credit reporting sector has been seeking moves in this direction for over ten years.

The ALRC's recommendations have been generally well received with one consumer group commenting that the "credit recommendations represent a fair, sensible and principled stance in the face of a massive and concerted campaign by the credit industry" and the Australian

Bankers Association saying that "ALRC has done an excellent job for the most part".[24] [25]

However, the approach worked out in the ARLC process is being challenged with some stakeholders saying the recommendations do not allow the collection of sufficient information to make a proper risk assessment.

Protection of a right to personal privacy

The ALRC has recommended that the Privacy Act should provide for a private cause of action where an individual has suffered a serious invasion of privacy, in circumstances in which the person had a reasonable expectation of privacy. It proposes that courts should be empowered to tailor appropriate remedies, such as an order for damages, an injunction or an apology. The ALRC's recommended formulation sets a high bar for plaintiffs, having due regard to the importance of freedom of expression and other rights and interests.

It recommendation is in part preemptive. It suggests that in the absence of a statutory provision the courts are in any event likely to proceed in this direction. It sees this outcome is likely to lead to inconsistent and fragmented privacy protection making it difficult for individuals to negotiate and for organisations, in particular media organisations to assess and manage their risk.

This set of recommendations has produced an aggressive response. In particular Australian media organisations see the proposals as a threat to freedom of expression and are signalling a strong campaign if these proposals proceed. The strength of the concern is surprising given that the ALRC's recommendation actually sets quite a high threshold before individual can commence an action, there must be: a reasonable expectation of privacy; and the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.[26]

The responsible Minister, Senator Faulkner, has indicated that this is not a priority area for implementation.[27] As the ALRC indicates, this will not prevent the courts from developing an approach if the issues are put to it.

Conclusion

The ALRC's recommendations, if adopted by the Government and legislated by the Parliament, are likely to produce a useful updating of the Privacy Act. Most significantly they potentially remove considerable complexity from the framework; although this could still be reintroduced via regulations and by the extensive reliance on guidance from the Privacy Commissioner to flesh out the changes. The refinements to the privacy principles for direct marketing and in relation to transborder data flows go to major issues of concern for individuals. Also very positive are the recommendations calling for the strengthening of the Act's enforcement provisions.

The ALRC inquiry has resulted in a valuable report offering an extremely detailed analysis of the operation of privacy law in the Australian context, including some of the current thinking on the concept of privacy and current privacy risks, and taking into account the views of a very wide group of stakeholders.

The insights offered into the operation of an existing privacy framework also have global relevance, the more so because the current frameworks are being questioned, for example in the context of research being funded by the United Kingdom Information Commissioner mentioned earlier, the current focus by the Asia Pacific Economic Conference on implementing its privacy framework and in calls by major US businesses for that country to adopt a comprehensive privacy law. [28] [29]

The question for the 21st century is going to be the durability of a framework that remains embedded in the thinking expounded in the 1980s by the OECD which is built on simple information flows and the notion of giving individuals control of personal information via the mechanisms of notice and consent. There is a growing sense that such notions are simply inadequate in the light of huge changes such as the Internet, the global movement of personal information and developments in information creation and use including behavioural marketing, business analytics and joined up government.

NOTES

[1] The ALRC's report is available at www.alrc.gov.au

[2] ALRC media release August 11, 2008 available at www.alrc.gov.au/media/2008/mr1108.html

[3] "Humans created 161 exabytes of data in 2006", iTnews.com.au, March 7, 2007, www.itnews.com.au/Tools/Print.aspx?CIID=74870

[4] "A New Approach to Trust and Privacy in the Information Age" - a paper for the *Privacy and Trust Partnership conference* convened in the Parliament House of NSW, Sydney, July 4, 2007

[5] For example, see a list of laws relating to the handling of personal information prepared by the Office of the Victorian Privacy Commissioner at http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/8219B55BB38A8CBBCA256F8C00209B48/$FILE/Privacy%20and%20related%20legislation%20in%20Australia%20at%2018%20October%202007.pdf

[6] See note 2 above

[7] The Privacy Act defines an interference with privacy as a breach of a privacy principle see s.13-13F of the Act at www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

[8] More detail on the history of the Privacy Act can be found on the Privacy Commissioner's website at www.privacy.gov.au and in the Australian Law Reform Commission's Issues Paper 32 Review of Privacy available at http://www.alrc.gov.au/inquiries/

[9] The key enforcement mechanism in the Privacy Act's private sector provisions is via individual complaints. While there is the option of formal determination enforced by the courts, most complaints are resolved by conciliation, sometimes including compensation.

[10] The two previous reviews were the: Parliament of Australia—Senate Legal and Constitutional References Committee, *The Real Big Brother: Inquiry into the Privacy Act 1988* (2005); and the Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005);

[11] ALRC Report 108 For Your Information: Australian Privacy Law and Practice, section 1, available at www.austlii.edu.au/au/other/alrc/publications/reports/108/1.html#fn1

[12] The full report is available at www.alrc.gov.au

[13] See Senator Faulkner's speech launching the ALRC report at www.smos.gov.au/speeches/2008/sp_20080811.html

[14] Themes not discussed in this article include: health services and research; children, young people and adults requiring assistance; telecommunications regulation; and fragmentation between the Privacy Act and other federal, state and territory laws.

[15] The full report is over 2500 pages and as noted includes 295 separate recommendations.

[16] See Chapter 10, note 12 above.

[17] See www.ico.gov.uk/upload/documents/pressreleases/2008/ico_leads_debate_070708.pdf and Note 4 above

[18] Professor Graham Greenleaf 19 August 2008 on *Australia Talks* www.abc.net.au/rn/australiatalks/stories/2008/2335577.htm

[19] See www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

[20] See "The Failure of Fair Information Practice Principles" by Professor Fred Cate in *Consumer Protection in the Age of the 'Information Economy'*, Amazon reference www.amazon.com/Consumer-Protection-Information-Economy-Markets/dp/0754647099

[21] Australian Chamber of Commerce and Industry 12 August 2008 Media Release available at www.acci.asn.au/text_files/media_releases/2008/77-08.pdf

[22] See for example, the Privacy Commissioner's functions as set out in sections 27-29 of the *Privacy Act 1988* and the powers to conduct investigations in section 42-47. The act is available at www.privacy.gov.au.

[23] See for example 'Light Touch' or 'Soft Touch' - Reflections of a Regulator Implementing a New Privacy Regime www.privacy.gov.au/news/speeches/sp2_04p.html

[24] Karina Barrymore (18 August 2008) Cracking the credit code *Herald-Sun*

[25] The Australian 12 August 2008

[26] See the ALRC report, recommendation 74.2 www.austlii.edu.au/au/other/alrc/publications/reports/108/74.html#Heading423

[27] Senator John Faulkner reported in *Don't die in the last ditch on privacy reform front* The Australian 14 August 2008

[28] See www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html

[29] For example see www.microsoft.com/presspass/features/2005/nov05/11-03Privacy.mspx