PRIVACY LAW REFORM: CHALLENGES AND OPPORTUNITIES

Timothy Pilgrim*

In May 2012 the Attorney-General announced major legislative reforms to the Privacy Act that will be achieved through amendments scheduled to be introduced into the Parliament in the winter sitting period. These include many of the changes anticipated since the Australian Law Reform Commission released its 2008 report into Australia's privacy laws, *For your information: Australian privacy law and practice.*

In making this announcement, the Attorney identified a number of consumer benefits as a result of these reforms. There will also be more powers for the Privacy Commissioner to resolve complaints, conduct investigations and promote privacy compliance.

While Australia's privacy framework may be undergoing reform, and while we may be witnessing revolutionary new technologies that are changing the way we think about the handling of personal information, community concern about privacy is a determined constant.

This quotation, for example, concerns community perceptions of privacy:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person….photographs and newspaper enterprises have invaded the sacred precincts of private and domestic life, and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house tops.[1]

Given recent media reporting of the impact of new technologies on people's privacy, incidents like the *News of the World* phone hacking scandal, and the imminent changes by Google to its privacy policy, you could be forgiven for thinking that this quotation is contemporary.

It is actually from the late 19th century.

These words were written by Samuel D Warren and Louis D Brandeis (who later became a US Supreme Court judge); they show the impact of the rise of the newspaper enterprise and of the emergence of new technologies, such as instantaneous photographs, on people's privacy.

The following are more recent comments, made by Mark Zuckerberg, the creator of Facebook:

> ...people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that has evolved over time. You have one identity. The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly. Having two identities for yourself is an example of a lack of integrity.

---

* *Privacy Commissioner Timothy Pilgrim presented this paper to the Emerging Challenges in Privacy Law Conference, 23 February 2012, several months prior to the May announcement.*

And, Scott McNeally, co-founder of Sun-Microsystems, famously said in 1999 that 'You have zero privacy – get over it'.

Privacy – a human right

How do such views, which it could be said are driven from the perspective of particular business models, sit with the concept of privacy as a human right?

I have no doubt that, innately, people continue to feel strongly about their right to have their privacy protected. That is why privacy is recognised as a basic human right, enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

At a time when Australia was signing as a party to the ICCPR, the late Sir Zelman Cowan delivered six lectures entitled *The Private Man* – as part of the ABC's annual Boyer lecture series. In one of these he observed that '… a man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars.'

The recognition of privacy as a human right, deserving of the protection of law, is one of the reasons we have the Privacy Act. Today, this is mainly the prism through which we view the concept of privacy. All too often, privacy is seen as an impediment to business practices or an administrative inconvenience—another box to be ticked on a compliance checklist. It is important to remember that privacy is a fundamental human right and is of key importance to the preservation of our free and democratic society.

Of course, we also recognise that privacy rights are not absolute – they must be balanced against other important rights and ideals, such as freedom of expression and national security.

Privacy law reform

In 2006, almost 20 years after the *Privacy Act 1988* (Cth) was introduced, the Government asked the Australian Law Reform Commission (ALRC) to conduct an inquiry into how well Australia's privacy framework was functioning.

In 2008, after significant public consultation, the ALRC concluded its inquiry with the release of its report, *For Your Information: Australian Privacy Law and Practice*, which contained 295 recommendations for reforms to the Commonwealth privacy regime. In the course of its consultations, the ALRC found that Australians care about privacy. They want a simple, workable system that provides effective solutions and protections. Australians also want the considerable benefits of the information age, such as shopping and banking online, and communicating instantaneously with friends and family around the world.

ALRC recommendations

While the ALRC report concluded that the Privacy Act had worked well, it proposed refinements to bring it up to date. These included:

- a new set of harmonised privacy principles to cover both the public and private sector;
- provisions introducing comprehensive credit reporting to improve individual credit assessments and supplement responsible lending practices;
- provisions relating to the protection of health information;

- a review of the exemptions to the Act;
- mandatory data breach notification; and
- a statutory cause of action for a serious invasion of privacy.

Given the significant size of the ALRC's report, the Australian Government decided to respond in a two-stage process. The Government released its first stage response to 197 of the 295 recommendations contained in the Report in October 2009, and is in the process of implementing these changes. These include the harmonised set of privacy principles, credit reporting and strengthening and clarifying the Commissioner's powers and functions.

Government's first stage response

The Privacy Law Reform agenda is ultimately the responsibility of the Government, not the Office of the Australian Information Commissioner (OAIC). In late 2011, the Government announced that, subject to its broader legislative program, it intended to introduce a Bill into Parliament during the autumn 2012 sitting, and that this Bill would include the Australian Privacy Principles, changes to credit reporting and a strengthening of the Commissioner's powers. [2]

We hope to see the Bill introduced soon. While the draft Bill hasn't been publicly released, we have seen exposure draft legislation of a number of the elements that the Government has said it will include. For example, there was wide consultation on the Exposure Draft of the Australian Privacy Principles (APPs).

The APPs will replace the two separate sets of principles which currently cover the public sector and the private sector in Australia. Having a consistent set of privacy principles covering business and government will simplify compliance obligations, particularly in the context of private sector contracted service providers to Australian Government agencies.

The changes proposed to the credit reporting provisions will allow for more comprehensive credit reporting. For example, it may be that the changes would allow credit reporting agencies to report on data sets, including credit limits on accounts, dates that accounts were opened and closed, and limited information on repayment history.

Commissioner's powers

In October 2009, the Government stated that it intended to give the Commissioner a range of new powers, including accepting enforceable undertakings and seeking civil penalties in the case of serious or repeated breaches. It also accepted the ALRC's recommendation that the Commissioner be empowered to make enforceable determinations following own-motion investigations.

No exposure draft legislation has been released in relation to what changes will be made to the Commissioner's powers at this stage. The former Minister for Privacy and Freedom of Information stated late last year that changes that would be included in the upcoming Bill would be likely to include new powers to approve external dispute resolution services and to implement the proposed new Credit Reporting Code of Conduct.

If the Commissioner is given stronger enforcement powers, this would have significant implications for privacy compliance in Australia. As the Privacy Act currently stands, we are unable to impose a sanction on an organisation when we have initiated an investigation on our own motion, without a complainant. Our role is to work with the organisation to ensure ongoing compliance and better privacy practice. Additional powers would provide added

credibility to the enforcement of privacy law, reinforce the significance of privacy compliance, and give departments and agencies an even greater incentive to take their privacy responsibilities seriously.

Overseas experience

Overseas experience indicates that regulators with the power to pursue large penalties will often do so. The United States is perhaps the best example of this. One notorious data breach in the USA was the disclosure by ChoicePoint, a large identification and credential verification organisation, of sensitive information it had collected on 145,000 individuals. A Federal Trade Commission investigation of this matter led to the imposition of a $15 million fine.

There have been many other breaches. Last year, Massachusetts General Hospital was fined $1 million for losing the medical records of 193 patients,[3] and in 2009, HSBC Bank was fined £3 million by the Financial Services Authority in the UK for failing to secure customer data.[4]

However, it is important to realise that privacy enforcement is about more than just financial penalties. In November 2011, the Federal Trade Commission (FTC) in the USA reached a settlement with Facebook over allegations of deceptive conduct in relation to its privacy practices. As part of the settlement, Facebook must obtain independent, third-party audits certifying that it has a privacy program in place that meets or exceeds the requirements of the FTC order every two years for the next 20 years. The FTC accepted an undertaking in similar terms in settlement of a matter involving Google Buzz earlier in 2011.

On the other hand, the French Data Protection Authority issued a €100,000 fine to Google due to breaches of French law caused by Google Street View. It is interesting to compare and contrast these approaches to enforcement. One wonders how effective a €100,000 fine would be for a multi-billion dollar organisation like Google.

Enforcement by the OAIC

Regardless of whether the Government decides to strengthen the Commissioner's powers, we have been changing our approach to privacy law enforcement.

In its current form, the Privacy Act only gives the Commissioner the power to make determinations on complaints received from individuals. In these complaints, we usually adopt a conciliation-focused approach.

However, for particularly serious privacy breaches or, for example, where conciliation is not achieving an outcome, we have demonstrated that we are prepared to use our power to make determinations directing how complaints should be resolved. Our determinations are enforceable in the Federal Court.

In late 2011, I held a hearing and issued the first determination made under section 52 of the Privacy Act in seven years. The determination arose from a complaint by an individual against a club.

The complainant gambled at the club. The complainant and the complainant’s ex-partner were engaged in child custody proceedings. The complainant's ex-partner provided the club with a subpoena requiring information about the complainant's gambling to be given to the court. Instead, the club gave the information directly to the complainant's ex-partner. The complainant alleged that this was an improper disclosure of their personal information. I

found in the complainant's favour. I determined that, to redress this matter, the club needed to:

- apologise in writing to the complainant within three weeks;
- review its training of staff in the handling of personal information and legal requests for personal information, including court subpoenas, and no later than six months from the date of this determination confirm that this review of training has been completed and advise me of the results of review; and
- pay the complainant $7,500 for non-economic loss caused by the interference with the complainant's privacy.

The full detail of the determination is available on the OAIC's website and on AustLII.

While it is still my focus to resolve most complaints via conciliation, I will not shy away from using my determination powers where it is appropriate to do so.

Determinations are important, not just because they provide an avenue for resolving complaints where conciliation fails but because they provide a public record of the OAIC's views on how privacy laws should be interpreted and can assist complainants and respondents to better understand how privacy laws will apply.

A number of other complaints are now in the process of determination.

The Office of the Information Commissioner is also changing its approach to particularly serious or high profile privacy incidents. The publication of investigation reports will increase the transparency of our investigation process and help organisations and agencies better understand their privacy responsibilities.

Four investigation reports are available on our website; they provide information about investigations into incidents involving Vodafone, Telstra, Sony and Professional Services Review.

The most recent report published was that concerning the Sony PlayStation Network investigation, which concluded in September 2011. We opened this investigation in the previous April after a media report stated that an unauthorised person accessed the personal information of approximately 77 million customers of the Sony PlayStation Network, including customers in Australia. It was alleged that individuals' names, addresses and other personal data, potentially including credit card details, had been compromised by the incident. Our investigation looked at Sony's data security practices.

We concluded that Sony had not breached the Privacy Act when it fell victim to a cyber-attack, because it had taken reasonable steps to protect its customers' personal information; this included encrypting credit card information and ensuring that appropriate physical, network and communication security measures were in place. However, while I found no breach of the Privacy Act by Sony, I was concerned about the time that elapsed—seven days—between Sony becoming aware of the incident and notifying customers and the OAIC.

Immediate or early notification that financial details have been compromised can limit or prevent financial loss to individuals, by enabling them to re-establish the integrity of their personal information. Evidence shows it can be very difficult for individuals to re-establish the authenticity of their identity when their personal information has been stolen and used fraudulently. I raised this concern publicly, both in a media release and in my investigation

report, by stating that I would have liked to have seen Sony act more swiftly to let its customers know about this incident.

While there is no requirement in Australian law for organisations to notify individuals or the OAIC of a data breach, I strongly recommended that Sony review how it applies the OAIC's *Data breach notification: a guide for handling personal information security breaches.*

The OAIC faced an interesting challenge in establishing whether it had jurisdiction to investigate this matter, due to Sony's corporate structure. We sought information from Sony Computer Entertainment Australia Pty Ltd. SCE Australia is a subsidiary of Sony Computer Entertainment Europe Limited (SCE Europe). A separate subsidiary of Sony Computer Entertainment Europe—Sony Network Entertainment Europe Limited—operates the PlayStation Network for individuals in Australia, holding their information in a data centre in San Diego, California.

The investigation involved a review of the acts and practices of both SCE Australia and the other Sony companies mentioned. As the incident occurred outside Australia, the Privacy Act only applies where the requirements of the extraterritorial application provisions in section 5B of the Act are met.

Section 5B of the Act prescribes that an act or practice engaged in outside Australia will be covered by the Act if that act or practice relates to personal information about an Australian citizen and the organisation responsible for that act or practice has an organisational or other link to Australia. Where an entity does not have an organisational link with Australia, the Act will only apply to the handling of personal information about Australian citizens where the organisation carries on a business in Australia and the personal information was collected by, or held by, the entity in Australia.

Whether the conduct of Sony Network Entertainment Europe falls under the jurisdiction of the Australian Privacy Act in this case is a complicated question. However, as the conduct in question by the Sony companies did not constitute a breach of the Act, we were not required to come to a settled view on jurisdiction.

In 2009–2010, organisations and agencies came to us on 44 occasions to report that they had been subject to a data breach. This increased to 56 in 2010–2011, and we are on track to receive a similar number in 2011–2012. We now receive more data breach notifications than we implement own-motion investigations. Increasingly, it is the organisation or agency subject to a breach rather than a tip-off or media report that brings our attention to these issues.

Industry is standing up and taking notice

Since the adoption of our new approach to privacy compliance, public commentary has indicated increased awareness by business of the need for compliance. Since my 2011 determination, we have noticed that some respondents have adopted a more proactive approach to conciliation of privacy complaints and have shown a greater willingness to offer compensation. So far, this is only anecdotal evidence gathered over a short period of time, but I think that it bodes well for the future of privacy compliance in Australia. The challenge to business and government in Australia is to ensure that privacy practices and procedures are rigorous, and that they will stand up to scrutiny if there is a data breach. All privacy complaints should be taken seriously.

Other challenges and opportunities

In the 1980s, when the Privacy Act was introduced, fax machines were still a relatively new addition to the office environment. The term 'hacking' meant having a bad round of golf. The commercialisation of the internet was still a decade away. The vast majority of filing was physical, and personal information was mostly held in paper records. Securing these documents was relatively easy—all you really needed was a lock and key.

In our modern world of cloud computing, portable storage devices, electronic databases and hackers, the parameters around data security and document storage have shifted immeasurably. All it takes is a single careless incident to cause a massive data breach. In the UK in 2007, two computer disks belonging to Her Majesty's Revenue and Customs were lost. The disks were thought to contain names, addresses, national insurance numbers and banking details of approximately 25 million people in the UK. A data breach on this scale would have been inconceivable when the Privacy Act was introduced.

The Sony incident, which I have already mentioned, involved hackers compromising records relating to 77 million people. Again, a breach of this kind could not have been imagined when the Privacy Act came into existence.

Data security has emerged as a major challenge for organisations and agencies. They must ensure that they have implemented robust information-security measures. However, data breaches can occur even when all reasonable steps have been taken to protect information. Organisations and agencies need to have contingency plans in place so that if a data breach occurs, they can deal with it swiftly, mitigating any risk of harm that the breach may cause.

While a data breach alone can cause reputational damage, recent experience shows that customers can be understanding if an organisation openly acknowledges a breach, apologises and acts promptly to resolve it. Greater reputational damage can occur if an organisation is seen to try to cover up a breach.

Communicating with clients about privacy is another key challenge for businesses. Too often, privacy policies are unwieldy documents, littered with legal jargon with which the average consumer is unable to engage.

In 2010, as an April Fool's Day prank, the British gaming retailer Gamestation.co.uk slipped an ‘immortal soul clause’ into its privacy agreement, knowing full well that most people would never read it. It was proven right—thousands of people unwittingly sold their souls to the company. My point is not that privacy policies are insignificant—this is far from the truth. The challenge for organisations is to ensure that their privacy policies are clear, relevant and easily understandable.

The importance of privacy policies is demonstrated by the recent example of Google; the company has recently reviewed its privacy policies. This policy (implemented in March 2012) includes some significant changes to the way Google interacts with the personal information of its users. These changes have caused significant public controversy and have attracted media attention. The OAIC is currently examining the privacy policy to determine whether it complies with the requirements of the Australian Privacy Act.

Globalisation of information flows is a particular challenge for privacy regulators. A company might be based in the USA, hold information in databases in Europe and provide services online to customers in Australia. If that information is compromised, it can be very difficult to establish which country's privacy regulator has jurisdiction to investigate the matter.

Australia's Privacy Act only applies to Australian organisations and to organisations with an organisational link to Australia. In the scenario mentioned above, it may be that the organisation concerned is not covered by the Privacy Act.

Privacy commissioners world-wide are working together to address this issue. For example, APEC economies have recently established the APEC Cross-border Privacy Enforcement Arrangement, under which privacy regulators can cooperate and share information to assist in the enforcement of laws in cross-border privacy matters. The Global Privacy Enforcement Network, established in response to an OECD recommendation, is an informal network that facilitates cross-border cooperation in the enforcement of privacy laws. A particular challenge in this area is that there are subtle differences between privacy laws in different countries. An act or practice that breaches one country's privacy laws might be lawful in another country.

Cross-border cooperation in privacy enforcement is still a relatively new concept, and I expect that, as we gain more experience in this area, we will unlock the opportunities presented by the prospect of greater global collaboration.

Regarding Google and the changes it is making to its privacy policy, members of the Asia Pacific Privacy Authorities Forum, which includes Australia and 11 other privacy enforcement authorities in the region, have asked its cross-jurisdictional Technology Working Group to review the changes. The Asia Pacific Privacy Authorities Forum has also been in contact with the European Union's Article 29 Data Protection Working Party about the changes. The French Data Protection Authority is investigating the changes on behalf of the Working Party. We will monitor developments in this area.

Finally, privacy law reform in Australia presents a number of challenges and opportunities. As well as the key aspects of the government's first stage response to the ALRC report—the APPs, credit reporting, and powers and functions—there are a number of other changes on the horizon. Once the Government has implemented its first stage response, it will move on to the second stage. This includes the prospect of mandatory data breach notification and consideration of some of the exemptions in the Privacy Act.

The Government released an *Issues Paper* on the introduction of a statutory cause of action for serious invasion of privacy in September 2011. It received more than 70 submissions from a variety of stakeholders. When or whether these reforms will take place is still not entirely clear, but depending on how the process unfolds, they could present both challenges and opportunities, as individuals, business and government come to grips with these new rights and responsibilities and take a further step in the evolution of privacy law in Australia.

Privacy awareness

Privacy Awareness Week is a joint initiative of the Asia Pacific Privacy Authorities – a group of 12 data protection authorities from countries including Mexico, the USA, Canada, Hong Kong, Japan and New Zealand.

The theme of Privacy Awareness Week in 2012 is *Privacy: It's all about you*.

This message is directed both at individuals and organisations. It reinforces the idea that individuals can take responsibility for their own privacy by taking some common sense steps, such as updating their privacy settings when they use social media, and not sharing passwords. It also shows that organisations have a responsibility to treat their customers' personal information with respect, by only collecting as much information as they actually need and by appropriately securing that information.

If you have not yet done so, I recommend you visit the Privacy Awareness Week campaign website at http://www.privacyawarenessweek.org. There you will find many educational resources that we encourage you to use, as well as all kinds of suggestions about how you can protect the personal information of others, as well as your own.

Endnotes

1 Louis Brandeis & Samuel Warren, '*The Right to Privacy*', 4 Harvard Law Review 193-220 (1890-91) http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

2 As mentioned in the first paragraph, a press release of 2 May 2012 by the Attorney-General states that this Bill will now be introduced into parliament in the winter sitting period of 2012.

3 http://www.infosecurity-magazine.com/view/16228/mass-general-takes-1-million-hit-for-losing-193-patient-records/

4 http://www.itpro.co.uk/613063/hsbc-fined-3-million-by-fsa-over-data-security