

THE PRIVACY ADVISOR

The Official Newsletter of the International Association of Privacy Professionals

iapp

Editor, Kirk J. Nahra, CIPP

January - February 2011 • Volume 11 • Number 1

Australia's changing privacy landscape



By Malcolm Crompton, CIPP

Since the Australian Law Reform Commission Report (ALRC) was tabled in 2008, we have seen the rise of the iPhone, iPad and a doubling of the users of Facebook, as well as an explosion in location-based services. And after a period of stability, Australian and international thinking about how best to protect citizen privacy is on the move.

The coming regulatory and environmental changes will mean different things for different businesses. For some, a more uniform regulatory framework that operates across borders, with lower costs and increasing consumer confidence in online dealings, will mean they can more easily take advantage of opportunities to grow online businesses inside Australia or in one or more other countries, or to use "cloud computing" to improve business efficiency. For others, it may mean that privacy compliance obligations have to be taken more seriously.

Without intending to be comprehensive, this background paper highlights some of the current regulatory, technological and social factors now affecting the privacy debate. The rate of change and privacy's place on the agenda are increasingly significant.

THE CHANGING PRIVACY REGULATORY LANDSCAPE

The ALRC Privacy Inquiry

In 2006, the attorney-general gave a new privacy reference to the ALRC. The reference was to assess whether the Privacy Act and related laws continued to provide an effective framework for the protection of privacy, taking into account the rapid advances in information, communication, storage and surveillance technologies and emerging areas that may require privacy protection.

The ALRC Report 108 [For your information: Australian privacy law and practice](#) was published in August 2008. Its three volumes and 295 recommendations aim for substantial reforms to the Privacy Act.

Government's Response to the ALRC Report

Given the large number of recommendations in the ALRC report, the government [decided](#) on a two stage response process. The 2009 first stage response outlined the government's position on 197 recommendations relating to

- developing a single set of privacy principles applicable to the public and private sectors;
- redrafting and updating the structure of the Privacy Act;
- addressing the impact of new technologies on privacy;
- strengthening and clarifying the privacy commissioner's powers and functions;
- the introduction of comprehensive credit reporting and enhanced protections for credit reporting information, and
- enhancing and clarifying the protections around the sharing of health information and the ability to use personal information to facilitate research in the public interest.

In June 2010, the government announced that it would be releasing draft legislation to implement the first-stage response in four parts. The first part was released at that time and set out draft Australian Privacy Principles (APPs) that would replace the IPPs and NPPs. The draft APPs are now being considered by the Senate Standing Committee on Finance and Public Administration, which has already [sought](#) submissions from the public and held initial hearings. Some of the more significant changes set out in the APPs include

- specific obligations to take steps to comply with the APPs and to document these in a privacy policy which is available on request;
- new obligations to tell people if personal information is to be transferred overseas, and
- changes in approach, including a greater focus on accountability, when disclosing personal information overseas.

The committee received 41 submissions that raise issues such as

- concerns about the structure and length of the APPs
- concerns, particularly from some privacy advocates, that the level of protection for individuals has been reduced in some areas such as the standards for collection, because of the extended use and disclosure exceptions and particularly in the approach to cross-border transfers, and
- concerns from private-sector organisations that the provisions are onerous, particularly in relation to: the new requirements to specify compliance; the direct marketing provisions; the requirements to advise individuals about the source of information when not collected from them and the countries to which information might be transferred, and in relation to the accountability requirements in the cross-border principle.

Next steps: A new Privacy Act – in Time

The new principles will be the cornerstone of a new Privacy Act. Apparently, it has been recently decided that a rewrite is called for rather than extensive amendment of the current act. As noted earlier, the first four parts, at least, are to be referred to a senate committee for consideration and public consultation as the drafting of each is completed. After the APPs, the next three areas for consideration will be

- credit reporting;
- health information, and
- the powers of the privacy commissioner.

The current timetable has the Senate Standing Committee concluding its report on the APPs before the end of the year. The legislative proposals for a new credit-reporting regime are expected to be released for consideration by the committee early in the new year, with draft legislation on the other two topics following soon after. The government would like the committee to have reported on all four parts by 30 June 2011.

The privacy commissioner, Timothy Pilgrim, has recently indicated that he thought the government hoped to introduce final legislation into parliament in respect of all these items prior to the end of the parliamentary sittings in 2011, although there was no guarantee that it would pass before the end of 2011. It is also not clear when the new legislation would take effect to replace the current legislation. While there was a gap of a year between passage of the private-sector provisions of the Privacy Act in 2000-2001, no decision has been taken as to whether there will be a transition period this time.

If this were not sufficient, a second parliamentary inquiry is under way into "The adequacy of protections for the privacy of Australians online," being conducted by the Senate Standing Committee on Environment and Communications. While notionally a narrower [brief](#), it is casting its net widely.

The slowing pace of the revision of the Privacy Act means that Australia risks falling behind just as the rate of change is beginning to accelerate in other important jurisdictions. While it is tempting to think that Australia should now go back to the drawing board, the very slow rate of the legislative process (which in this round started in 2006 and is not likely to see fruition until 2012) suggests strongly that we should proceed with the current revisions of the Privacy Act and then go on from there.

Global Trend—Strengthening Privacy Enforcement and Increasing Regulator Enforcement

The changes to Australia's privacy law come at a time when there are global calls for stronger enforcement of privacy laws and for greater cooperation between privacy regulators. It is also evident that lawmakers and regulators as well as business and community interests are very aware of the need to find ways to harmonise and integrate the disparate privacy regimes now operating across the world.

Without attempting a comprehensive survey or analysis, some of the recent developments and commentary include:

- A range of informal arrangements for mutual assistance has been made to strengthen the enforcement of domestic privacy laws in the context of international data transfers. These include the [Asia-Pacific Privacy Authorities Forum](#) (APPA), a formalised secretariat arrangement for the annual International Conference of Data Protection and Privacy Commissioners (ICDPPC) and the new [Global Privacy Enforcement Network](#) (GPEN). These forums and arrangements acknowledge the need for structured information sharing and cooperation among regulators in the management of privacy risk. For example, the GPEN was established after the OECD Council adopted a [Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy](#), which provided that "member countries should foster the establishment of an informal network of privacy enforcement authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness-raising campaigns." The ICDPPC adopted a similar [resolution](#) in 2009.
- At the same ICDPPC conference, a group of international companies including Oracle Corporation, Microsoft Corporation, Google, Inc., and Hewlett-Packard Company welcomed the initiative of the International Conference of Data Protection and Privacy Commissioners to [explore](#) frameworks for better global coordination of [privacy regimes](#).

- A recent report, "New Era of Compliance: Raising the Bar for Organizations Worldwide," written by RSA and the Security for Business Innovation Council, [analyses](#) how new legislation and more legal muscle behind regulations are forcing businesses to change how they approach compliance.
- Remarks by Peter Hustinx, the European Data Protection Supervisor, [indicating](#) that he sees the future based on implementing stronger incentives to do the right thing by privacy—and commercial reality plus regulatory incentives—and really getting privacy right: not just seeking compliance with privacy law but demonstrating that "all measures have been taken to ensure that compliance will be a result."
- Ten data protection authorities from around the world [say](#) Google, Inc., and other international corporations are overlooking privacy values and legislation when they launch new online products.

The APEC Privacy Framework

One of the most significant examples of the trend to globalisation of policy and enforcement cooperation has been the development and implementation of the [APEC Privacy Framework](#). It has great potential as a mechanism for many Australian businesses to meet their privacy law obligations when trading across borders.

The framework responds to the considerable variety of approaches to privacy protection between APEC member economies, and indeed between economies around the world. It deals primarily with personal information as it moves across borders between APEC member countries, but it also aims to build privacy capacity within APEC domestic economies.

Rather than attempt to achieve a uniform privacy approach across economies, the APEC Privacy Framework is providing a minimum benchmark for privacy protection in the domestic context and a cross-border framework that is initially based on allowing companies to develop Cross Border Privacy Rules (CBPRs) that meet minimum requirements and are enforceable. To achieve this, the CBPR framework includes

- a baseline set of privacy principles as the minimum standard (which would complement but not displace any existing higher country standards);
- assurance, based on business "self assessment" confirmed by independent third-party "accountability agents," that participating businesses have adopted at least the minimum set of privacy principles and have processes in place to implement the principles;
- easy and effective mechanisms for individuals to pursue remedies if things go wrong and that assure individuals that the privacy protection they enjoy within their country will follow personal information as it is handled by businesses in other countries;
- a governance mechanism to ensure the system is transparent, accountable and working well, and
- backstop protection by regulatory bodies within a country and cooperation between regulators across borders (formalised recently by the [APEC Cross-border Privacy Enforcement Arrangement](#) (CPEA)).

The Australian government has been a strong supporter of the APEC privacy work. It sees the potential in the approach, as set out in the privacy framework and now soon to be implemented with CBRS and enforced in part through the CPEA, as a way of maintaining the privacy protections individuals enjoy within their own country in cross-border trade as well as encouraging the development of domestic laws where they are not in place.

Australia is one of five countries that have signed up to the CPEA. Amongst other things this means it could disclose information about Australian privacy investigations to other regulators (provided this is consistent with the Privacy Act). It is also taking the opportunity raised by current proposals to the Privacy Act to provide for a company's CBPRs as a possible way to satisfy the Privacy Act requirements to protect personal information be disclosed outside of Australia.

OTHER CHALLENGES AND DEVELOPMENTS IN THE REGULATORY ENVIRONMENT

Privacy Principles—Some New Approaches Needed

Traditional privacy principles are based strongly on the notion of people being in control of personal information about them. Privacy notices and individual consent were thought to be effective mechanisms to give people control. This thinking is now being challenged. Behavioural economics is being recognised as significant in developing privacy frameworks and enforcing them. It examines how people actually respond in practice. It has shown that assumptions behind common privacy frameworks are not working as expected. Individuals do not read notices while consent when widely used becomes meaningless. Other models, for example, incentives and privacy “nudges,” can be effective. Data breach notification requirements implemented over the last decade have proved to be a powerful nudge. The setting of privacy defaults (e.g. opt in versus opt out arrangements) is also critical.

ID Management

The solution to effective and acceptable ways for individuals to identify themselves and to be identified online is still elusive, but there is now a range of approaches emerging. Information Integrity Solutions (IIS) introduced the issues in a [paper](#) prepared for the most recent ICDPPC held in October in the following terms:

The need to create trust and security in the digital world is currently a preoccupation of governments and private-sector organisations globally. The digital world and the Internet in particular were built on the assumption that using the Internet was almost risk free. It was originally developed to be a closed environment, and the information exchanged did not need protection or sharing restricted. As a consequence, mechanisms to manage risks, such as a trust framework, were not built. A key element missing was any means of identifying who was connecting with whom. In the absence of mechanisms to establish trust in the digital world and in the face of rapid expansion and the increasing value and availability of information about people, the criminal element has moved in. There has been increasing concern that there could be a major trust crisis that might threaten the vibrant digital economy.

The paper identified themes including: usability (enrollment, multiple credentials, control); privacy (control and information limitation); interoperability, and two-way trust. It canvasses and assesses a range of solutions currently available.

Cloud Computing

In simple terms, cloud computing is a way to enhance computing experiences by enabling users to access software applications and data that are stored at off-site datacentres rather than on the user’s own device or PC or at an organisation’s onsite datacentre.

The National Institute of Standards and Technology, Information Technology Laboratory [considers](#) that there are a number of versions of the cloud with different characteristics, and therefore different risks. It considers that:

*Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**.*

The properties of cloud computing do raise questions about security and privacy, such as

- whether hosted data and applications within the cloud will be protected by suitably robust privacy policies;
- whether the cloud computing provider's technical infrastructure, applications, and processes are secure, and able to meet privacy law obligations to take reasonable steps to protect personal information and to protect it from loss or unauthorised access;
- where the information will be stored—in Australia, or in another country and can privacy obligations be met when data is moving across borders, and
- the processes to support appropriate action in the event of an incident that affects privacy or security.

In Australia, these questions are tending to limit extensive take up of some cloud services, particularly when the service is hosted outside of Australia.

Privacy by Design

Since Ontario Information and Privacy Commissioner Ann Cavoukian first developed the concept, it has become the new framework for thinking globally. Leaders in the European Commission, the European Data Protection Supervisor, the UK Information Commissioner and interests in the U.S., such as the Department of Commerce, all see great promise in this way of ensuring privacy is “built in” rather than “built on” later as a compromise.

A number of recent initiatives in Australia have included Privacy by Design as part of more comprehensive strategies to respect privacy. These include the health identifier being issued for all Australians.

The following points drawn from the Ontario Commissioner's Web site give a brief overview of the concept. There is a wealth of material on Privacy by Design at <http://www.privacybydesign.ca/>.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Principles of Privacy by Design may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of Privacy by Design—ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage—may be accomplished by practicing the following 7 Foundational Principles, which are

1. *Proactive not Reactive; Preventative not Remedial*
2. *Privacy as the Default*
3. *Privacy Embedded into Design*
4. *Full Functionality—Positive-Sum, not Zero-Sum*
5. *End-to-End Security – Lifecycle Protection*
6. *Visibility and Transparency*
7. *Respect for User Privacy*

Transatlantic Thaw

A feature of the privacy environment in the last 20 years has been significant differences in approach by the European countries and the United States. Some have described this as the tension between an “inalienable rights” approach coming out of Europe and the U.S. model, which is more consumer-protection focused and where the primary need is seen to be to adapt privacy regulation to accommodate new business models so as not to stifle innovation and economic growth (and not to interfere with free expression).

The last couple of years has seen a significant thaw with both the EU and the U.S. being much more willing to understand and see value in each others’ perspectives; the meeting point seems to be a recognition that neither approach has succeeded in delivering privacy outcomes for citizens.

This “thaw” is likely to be a significant contributor to strong global enforcement and to any changes in privacy law. It is likely to lead to more alignment in principles and rules and more cooperation.

Right To Be Forgotten

An emerging trend in the privacy debate in the online environment is the concept of the right to be forgotten. The following extract from a *New York Times* [article](#) gives an idea of the issue.

In a recent book, Delete: The Virtue of Forgetting in the Digital Age, the cyberscholar Viktor Mayer-Schönberger cites Stacy Snyder’s case as a reminder of the importance of “societal forgetting.” By “erasing external memories,” he says in the book, “our society accepts that human beings evolve over time, that we have the capacity to learn from past experiences and adjust our behavior.” In traditional societies, where missteps are observed but not necessarily recorded, the limits of human memory ensure that people’s sins are eventually forgotten. By contrast, Mayer-Schönberger notes, a society in which everything is recorded “will forever tether us to all our past actions, making it impossible, in practice, to escape them.” He concludes that “without some form of forgetting, forgiving becomes a difficult undertaking.”

Google’s Eric Schmidt [put](#) an irreverent view on the solution.

In August, Schmidt famously told The Journal that every young person will be entitled to automatically change their names when they reach adulthood in order to escape all the embarrassing stuff they did on social networking sites.

A more serious proposal comes from the EU’s Rights Commissioner, Viviane Reding, who [said](#),

“Internet users must have effective control of what they put online and be able to correct, withdraw or delete it at will. What happens if you want to permanently delete your profile on a social networking site? Can this be done easily? The right to be forgotten is essential in today’s digital world.”

It is not yet clear how viable the right to be forgotten concept will be. Certainly, as an absolute right it is doomed to fail. There are clearly classes of personal information—in the health, finance, law enforcement areas for example—where retention of information is crucial. However, perhaps a more nuanced approach will have some value and efficacy.

CONCLUSION

After a relatively quiet period in the debate about how personal information should be protected, in the last year the debate has accelerated and become a lot more visible. Two trends have contributed. First, some notable developments in technology and the response of policy makers and regulators. While the environment is perhaps

less “stable,” the direction is clear—not one jurisdiction has repealed its privacy law, while many have introduced such law recently.

In the next few years, we can expect a rewritten Privacy Act in Australia, significant developments if not new law in the U.S. and Europe to protect personal information and a significantly greater expectation that privacy regulators find a way of reaching across borders effectively to deliver that protection. The latter will be a combination of new law but also additional funding and stronger public expectation supported by lawmakers.

That said, the slowing pace of the revision of the Privacy Act means that Australia risks falling behind just when the rate of change is beginning to accelerate in other important jurisdictions.

Companies that can improve their capability to demonstrate that they are accountable for their handling of personal information and can “bake in” Privacy by Design will be the ones with the long term winning strategy. In the short term, it will pay well to follow the privacy policy debate in Australia and to contribute to it.

Malcolm Crompton is the managing director of Information Integrity Solutions Pty Ltd. He is the former Australian privacy commissioner and current member of the IAPP Board of Directors.