Lost in the Landscape of Australian Privacy Regulation

Peter Leonard shines a light on the regulatory landscape in which privacy professionals and their lawyers have to operate.

Finding your bearings in the Australian privacy landscape has become increasingly difficult.

It has become even more challenging to explain the landmarks to people who are privacy professionals. The first challenge is to explain that the Australian Privacy Commissioner sits in the Office of the Australian Information Commissioner (**OAIC**) and applies laws that the Australian Parliament has misleadingly and deceptively elected to call 'principles'.

The second challenge is describing how to read principles as laws and how to fit them together with other provisions in the *Privacy Act 1988* (Cth) (the **Act**) that clearly are laws. Then try to apply them as fit for the purpose of dealing with exotica like cross-border cloud deployment, cross-border access to personal information held in another jurisdiction (or jurisdictions unknown), geo-tracking of devices, data warehouses, virtualised servers, big data and customer data analytics.

From 12 March 2014, Federal privacy law will require organisations to devise technical, operational and contractual safeguards to implement privacy and security by design.

Third is the challenge of explaining how, from 12 March 2014, privacy and security by design will become law (through principle drafted in very general terms that never refer to these concepts). If you cannot point to a clear statement of the law, how do you explain that privacy and security must be built into the architecture of information flows and the engineering of how organisations structure their processes and design their products? From 12 March 2014, Federal privacy law will require organisations to devise technical, operational and contractual safeguards to implement privacy and security by design. However, industry practice has not yet developed to the stage where we can reliably say what safeguards are appropriate, implemented how, or when.

Scepticism often sets in when management is told that this is not just a case of bolting on additional technical security to existing information and work flows. Incomprehension usually arrives when the information engineers and the privacy and compliance professionals gather together and the engineers hear that their best practice security risk management frameworks and methodologies do not really work for personal and sensitive information. And, by the way, all that information about customers that looks innocuous and 'everyone must know' really is regulated personal information about individuals.

Next is the challenge of explaining the legal status of the 'guidance' from the OAIC, particularly in an environment where the Australian Parliament dodges hard issues by placing increasing reliance on OAIC guidance as to principles (law) to give context and meaning to law (without giving this guidance any formal legal status).

A further challenge is that although the Privacy Commissioner has a central guidance and enforcement role, it has been allocated very limited staff and other resources, despite a major expansion in the Commissioner's responsibilities and the importance of privacy throughout the Australian economy. Given the importance of the Commissioner's guidance on key matters about the application of the new privacy laws from 12 March 2014, one really cannot expect the Commissioner, when allocating a meagre budget and limited staff, to have much to say about the gazillion privacy policy issues exercising privacy regulators and privacy professionals around the globe. On top of this, the Commissioner must also address major government privacy issues, such as data sharing between government agencies and cloud computing. And deal with PRISM. And just wait until the industry codes start arriving on the Commissioner's desk.

Privacy regulation also pops up in lots of different places in Australia nowadays. In addition to the OAIC interpreting and applying the Act, the Australian Communications and Media Authority (the **ACMA**) has become a very active privacy policy maker. First, by applying its Privacy Guidelines for Broadcasters in investigations about privacy related infractions of broadcasting codes, the ACMA has been the chief developer of the law as to serious invasions of personal privacy involving the electronic media. Although we do not yet have an accepted private right of action for invasion of privacy in Australia, the ACMA has developed and applied rules as to what is a serious invasion of personal privacy. Second, through the ACMA's application of the Telecommunications Consumer Protections Code C628:2012 (the **TCP Code**), the ACMA has become a principal regulator of the handling and use of telecommunications related personal information. The TCP Code has strong privacy provisions which require telecommunications service providers to, among other things, have robust procedures to keep customer personal information secure. These provisions have been applied against communications providers for failing to adequately secure stored customer information from third party hack-in intrusions.

The ACMA has also been a vigorous enforcer of spam and do not call legislation, two key planks in the regulation of electronic marketing. It has used its research and policy budget to good effect, actively blogging on its new website and recently releasing a series of detailed discussion papers on diverse privacy related topics, such as why 'coherent regulation is best for digital communications policy', cloud services, near field communications and apps. These papers include proposals for an active role for the ACMA in the further development of privacy regulation of all information passing through telecommunications links, over radiocommunications or derived from communications services. In an interconnected digital and cloud based world, that is most information.

But that is not all.

We also have the Australian Competition and Consumer Commission applying the Australian Consumer Law. In the United States the Federal Trade Commission has used comparable laws to become a de facto regulator as to the fairness and intelligibility – or in the trendy, new term, 'transparency' – of privacy statements and consumer contracts. These laws are also powerful tools for the regulator to argue that if a corporation does not comply with its own privacy statement, that corporation is guilty of misleading or deceptive conduct.

We have the Australian Attorney-General's Department applying the poorly understood *Telecommunications (Interception and Access) Act 1979* (Cth) and Federal Criminal Code provisions relating to unauthorised access to stored communications – such as email servers – and other unauthorised access to information technology systems. Arguably many cookie deployments today infringe these provisions.

We have State and Territory Governments and regulatory authorities applying State and Territory privacy laws relating to personal information collected by State and Territory agencies, use of workplace or video surveillance technologies, use of tracking devices and technologies and access to computer data. And a diverse range of health information privacy laws with purported reach to the private sector, including entirely standalone restrictions on cross-border transfers of health related information. There is plenty of little understood overlap of State and Federal law, and plenty of variation in the State and Territory laws.

And then, of course, there are many industry codes of practice, many of which include provisions dealing with privacy and provide remedies for non-compliance.

So privacy and data protection in Australia has become a confusing landscape, with forests of regulation to get lost in, unexplored corners and poorly signposted and potholed roads. At a time when privacy and information security is becoming a major area of concern for governments, businesses and citizens, it is unfortunate that Australia has created such a confusing thicket of regulation and quasi regulation.

although the Privacy Commissioner has a central guidance and enforcement role, it has been allocated very limited staff and other resources, despite a major expansion in the Commissioner's responsibilities and the importance of privacy throughout the Australian economy

So the next time that the CIO chairs a security and privacy compliance meeting with the CMO, the HR director, the information security experts and the privacy professionals, and that meeting disappears into a cloud of mutual incomprehension, you'll understand why.

Peter G Leonard is a Partner at Gilbert + Tobin Lawyers and iappANZ Director. An earlier version of this article has been published in the iappANZ Members Newsletter.