PRIVACY – A REGULATOR'S PERSPECTIVE

John McMillan*

Privacy issues are both frequent and prominent in the daily media. A common link is privacy, technology and big data. In the news today, for example, there are stories about traffic cameras being used for mass surveillance, health and lifestyle information stored on smart watches being unsecured, the hacking of the Ashley Madison dating website, and retail photo booths linking credit card information to stored names and images.

The concept of privacy and how it is threatened is continually expanding. Privacy was famously defined by Warren and Brandeis in 1890 as the right 'to be let alone'.[1] A particular threat they had in mind was that a person's private affairs could be dragged into the public arena against their will by new developments such as photography and newspapers. In a later age with different threats, Cowen in the Boyer Lectures in 1969 saw privacy as the right of individuals 'to secure autonomy in at least a few personal and spiritual concerns, if necessary in defiance of all the pressures of modern society'.[2]

Those definitions no longer capture the spread of interests that now fall within the concept of privacy: as the Australian Law Reform Commission observed in 1983, 'privacy is a collection of related interests and expectations, rather than a single coherent concept'.[3] Nevertheless, the core principle on which the 'right to privacy' rests has changed little over time. It is that individuals should have control over when and how their personal information is released into the public domain.

Undoubtedly that is now a more complex challenge. Many privacy breaches involve the unauthorised release of or access to personal information that an individual has already shared with others – such as a bank, an employer, a government agency, the phone company or the operator of an electronic gate. The information sharing was done for a particular purpose and the individual did not expect that their personal information would be used or released for a different purpose. There was no general surrender by the individual of their right to decide when and with whom their personal information could be shared.

This more nuanced concept of privacy is reflected in the thirteen *Australian Privacy Principles* (APPs) that commenced operation in 2014 as part of a remodelled *Privacy Act 1988*. The APPs regulate the collection, use, disclosure, management, access to, amendment and destruction of personal information. They do so in a detailed manner: there are special rules for particular categories of personal information such as credit and health information; there are listed exceptions to every privacy principle; the APPs extend to cross-border sharing of personal information and to personal information stored in 'cloud' facilities housed in other countries; and the APPs address new privacy challenges such as direct marketing and data matching.

* Professor John McMillan was Australian Information Commissioner at the time of this presentation.

The other notable feature of modern privacy law is that administration and enforcement is placed in the hands of an independent privacy regulator, presently the Office of the Australian Information Commissioner (OAIC). The regulatory functions, responsibilities and powers of the OAIC were enhanced in the 2014 reforms. They include complaint investigation, the award of compensation, commissioner-initiated investigations, providing guidance on privacy law, monitoring and assessing compliance by entities to which the law applies, directing a government agency to undertake a privacy impact assessment, requiring an enforceable undertaking by an entity to comply with the law, bringing proceedings to enforce an enforceable undertaking, and applying to a court for a civil penalty order of up to $1.7M for a breach of a civil penalty provision.

The development and expansion of privacy law and regulation reflects the growth and value of personal information. Ninety percent of global data was generated in the last two years, and it is forecast that the amount of data globally will continue to grow by about 50% each year. Not all data is personal information, but a high proportion is. One estimate is that over 80% of information stored by government is linked to a residential or business address. An apt description of personal data by the European Consumer Commissioner is that it is 'the new oil … the new currency of the digital world'.[4] Reflecting that value, the global giants of a former age (Exon, Mobil, Texaco, BP) have largely been overtaken by the new information resource giants (Microsoft, Google, Facebook, Apple, Yahoo, LinkedIn).

The value of personal information has been substantially enhanced by data analytics. This is the process by which large quantities of personal data can be amassed, aggregated, analysed, reassembled, shared and put to different uses. The profound benefits in this process belong not only to the corporate data custodians, but to individuals in transactions as routine as electronic banking, online shopping and search-engine research. We benefit too through the greater capacity of government to understand the economy and society and to forecast the impact of government regulation and the working of the tax and transfer system.

The privacy debate now intersects with an expanding variety of public agenda issues, as diverse as counter terrorism, use of telecommunications data, aerial drones, biometrics, the e-health system, downloadable apps and credit regulation. The role of the regulator is principally to ensure that compliance with the Australian Privacy Principles is a paramount concern in those and other developments. That rests on a key definitional issue: whether the data that is being managed is 'personal information' to which the Privacy Act applies.

That term is defined in the Act as meaning 'information or opinion ... about an individual who is reasonably identifiable'.[5] In an earlier age, the more obvious information to which that definition applied was a person's name, photograph and residential address. In a digital age the definition can extend more broadly to information that can reasonably be used to trace a person – such as an email address, credit card information, or a telephone number. Data analytic capacity adds a new dimension altogether, since it enables items of data that bear no identifying mark to be assembled in a mosaic that does identify an individual.

This is a prominent issue in a recent ruling of the Privacy Commissioner, Timothy Pilgrim, in a case in which a Telstra customer sought access under the APPs to the customer metadata it held relating to his mobile phone usage.[6] The metadata was spread across Telstra's networks and records management systems. A person outside the organisation with access to the metadata would probably not be able to identify the customer. Telstra, on the other hand, had the operational capacity to identify the applicant because of its advanced systems for aggregating and reading the data. Accordingly, the Commissioner ruled that the applicant was to be given access to the metadata – his personal information – as required by the APPs.

The decision brings into sharp relief the choices and tensions that now arise in privacy law. On the one hand, the outcome in this case has been applauded by some who see it as a realistic recognition that data analytics has changed the landscape by enabling inconsequential and anonymous data to be used to identify individuals. It is appropriate, it is argued, that privacy law should apply to that data in order to safeguard individuals who would otherwise have little control over how the data is used and managed. The data has been acquired for corporate use for the sole reason that it is valuable and supports the commercial enterprise of the organisation that holds it. There should be corresponding responsibilities in managing a valuable, sensitive and potentially damaging resource.

The opposing argument is that privacy law is being stretched well beyond its central purpose. The anonymous data is not personal information in any popular sense. Telstra alone may be the only organisation with the capacity to use it to identify an individual. The risk of misuse of the data can be controlled in other and more appropriate ways. To apply privacy law to data of this kind is to impose responsibilities that are unrelated to any genuine risk of mismanagement. Classifying anonymous data as personal information mean that all the APP rules have to be observed on matters such as privacy management plans, collection notices, access arrangements and destruction schedules.

Another arena in which a similar debate is now being played out is in relation to recent legislation that requires telecommunications providers to retain data for two years so that it can be accessed by law enforcement agencies for national security purposes.[7] The public debate focussed strongly on whether this practice posed an unacceptable danger to privacy. The Government pointed to the safeguards in the legislation, including strict statutory controls around the retention and disclosure of this data, and OAIC and Ombudsman oversight of whether those controls were being observed. There was also a Government attempt, largely abandoned once the debate began in earnest, to argue that the privacy impact was minimal because the law only required retention of telecommunications metadata, and not the content of messages.

Critics responded that it may be more worrying from a privacy perspective to know who was called and at what time, than what was said in the call. The other strong criticism of the data retention legislation was that it had blanket application to all telecommunications metadata and could go well beyond the stated purpose of enabling detection of terrorism-related activity.

An OAIC proposal that was adopted in the legislation is that telecommunications data to which the law applies is deemed to be personal information. This will ensure that it is managed in accordance with the APPs and under the regulatory oversight of the OAIC – an important privacy development.

Another important Government concession during the data retention debate is the need for a mandatory data breach notification scheme.[8] At present there is a voluntary scheme administered by the OAIC, that urges organisations to notify consumers and the OAIC if a serious data breach occurs and of the steps being taken to remedy the privacy breach.[9] Some organisations take this voluntary step, but many others will try actively to suppress public knowledge of a breach for reputational reasons. The underlying principle of privacy law – that individuals should have control over when and how their personal information is released into the public domain – presupposes that people should know how their personal information is being managed and if a serious privacy breach occurs.

Privacy law now imposes considerable legal and administrative responsibilities on data custodians. Being aware of what is required and taking proactive steps to comply – captured in the universally popular phrase, ‘privacy by design’ – is the most constructive way of

reducing the compliance and regulatory burden. Three other options that can alleviate any burden – and that are strongly promoted by the OAIC – are to de-identify or anonymise data, to provide individuals with online access to their personal information, and to undertake a privacy impact assessment when designing a new program.

The first option – de-identification – can effectively remove data from the operation of the Privacy Act. The Act applies only to 'personal information'; information that has successfully been stripped of personal identifying qualities will no longer fall within the regulatory requirements of the APPs. At a transactional level, organisations should continually question whether, for example, they need form fields that require the entry of personal information. This should be accompanied by an active record review and destruction process to ensure that personal information is not retained for any longer than it is required for genuine operational purposes.

The benefit of the second option – online access – has been demonstrated by financial institutions that provide customers with online access to their own account. The customer can view, update and remove items of information. The regulatory burden on the organisation is substantially reduced, along with the suspicion that personal information may be misused by the organisation. The practice of providing individuals with access to their own personal information is one that should be adopted more widely by organisations.

The third option is to undertake a privacy impact assessment at the design stage of a new program. Consideration should be given to involving or consulting other stakeholders who may have relevant experience or interest – such as customers, IT security consultants, and privacy professionals. A privacy impact assessment provides an excellent opportunity to take stock of the types of personal information that is being collected, how it will be managed, breach risks, the response strategy if a breach occurs, and the record destruction schedule.

I will finish with an observation on one of the common fallacies that is often raised about privacy regulation. What is the purpose of privacy laws, some argue, if the largest global data custodians – the social media giants – can thumb their nose at them? While social media trends have rightly attracted considerable public comment and criticism, the reality is that the main corporate players are earnestly attuned to the need for good privacy practice. Their business model depends entirely on having the regulatory freedom to amass and use personal data, and their commercial survival depends on individuals entrusting personal information to them. There is room for differing views on whether social media giants should reveal more about their data management practices and whether more limitations and safeguards should be in place, but the corporate players actively engage on these issues with privacy regulators around the globe.

Financial institutions have similarly understood and adopted the mantra that good privacy practice is good business sense. Interestingly, on the most recent consumer awareness study undertaken by the OAIC,[10] people placed higher trust in financial institutions to manage their personal information than in other commercial or government agencies. This consumer trust has been built in an era when financial institutions have been amassing and using more customer information.

Privacy law and practice is now an area of great importance and complexity. The regulatory role in this area becomes ever more active.

Endnotes

1 S Warren and L Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193, 195.
2 Z Cowen, *The Private Man* (ABC, 1969) 10.
3 ALRC, *Privacy*, Report No 22 (1983), Vol 2, [1032].
4 Cited in Andreas Busch, 'Privacy, Technology and Regulation' in B Roessler & D Mokroinska (eds), *Social Dimensions of Privacy: Interdisciplinary Perspectives* (2015) 312.
5 *Privacy Act 1988* (Cth) s 6.
6 *Ben Grubb and Telstra Corporation Limited* [2015] AICmr 35. The Commissioner's decision was later set aside on appeal by the Administrative Appeals Tribunal, on the basis that the relevant information was not information about an individual: *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991. The Commissioner has appealed the AAT's decision to the Federal Court.
7 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*; see also *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act 2014.*
8 The Government commenced public consultation on an exposure draft bill in 2016: www.ag.gov.au/consultations/pages/serious-data-breach-notification.aspx
9 OAIC, *Data breach notification – A guide to handling personal information security breaches*.
10 OAIC, *Consumer attitudes to privacy survey*, Research report (2013).