Privacy and Self-management Strategies in the Era of Domestic Big Data

Xavier Fijac considers the value of a rights-based approach to privacy in the digital age.

Instantaneous photographs and newspaper enterprise 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 rooftops'.[1] *- Warren and Brandeis (1890).*

As Warren and Brandeis' 120 year old quote shows, privacy fears surrounding the introduction of new and invasive technologies often fail to be matched by reality. However, the issue for the contemporary period is that privacy concerns about private information being 'proclaimed from the rooftops', are being replaced by concerns about more permanent records such as the massive amounts of personal data being tracked and recorded via social media networks. Emerging technologies such as Facebook's 'Graph Search' point to the domestication of the kinds of powerful information analysis tools normally associated with 'big data', suggesting such fears may in fact be relatively well-founded. This article considers what the recent decision not to introduce a statutory right to privacy might mean for Australians hoping to protect their privacy from each other in an increasingly data-soaked world.

The Australian Government recently passed major reforms to the *Privacy Act 1988* (Cth), increasing the statutory requirements imposed on organisations dealing with personal information. However, the Government rejected the recommendations of the ALRC and decided against the introduction of a statutory cause of action for personal privacy invasion. Such a reform would have given individuals a right to privacy enforceable in the civil courts, and would bring individual privacy rights closer towards the existing rights-based protections in comparable jurisdictions around the world.[2]

The lack of a tort for privacy invasions has been described as a 'clear gap' in the privacy landscape, leaving individual Australians without legal redress for serious, and even more casual invasions of their privacy.[3] However, some 100 years after the introduction of privacy rights in the US, leading American privacy scholars have begun to question whether a rights-based approach to privacy protection is an effective way to address privacy issues between individuals.[4] It is therefore worth asking whether holding out for an Australian cause of action for privacy invasion is in fact the best way to address mounting privacy challenges in the age of domestic data surveillance.

Having never recognised a stand-alone right to privacy, the Australian approach to privacy management has traditionally been characterised by the 'self-management' approach articulated in *Victoria Park Racing*.[5] This puts almost complete emphasis on personal responsibility and pro-active protection of an individual's privacy rather than the exercise of specific privacy rights. As Latham CJ expressed it, an individual wanting to protect themselves from the prying eyes of their neighbours could simply 'erect a higher fence'.

Since the High Court's 2001 *Lenah Game*[6] decision, judicial attitudes appear to have shifted towards what has been described as a 'rapidly growing trend towards recognition of privacy as a right in itself deserving protection'. While this appears to reflect the current position of the courts, there is little doubt that both technology and public concerns about privacy are developing much faster than the common law. However, the logical conclusion to be drawn from the Government's recent refusal to recognise a statutory right is that the self-management or 'erect a higher fence' model remains ingrained in Australian legislative policy at some level.

Emerging technologies such as Facebook's 'Graph Search' point to the domestication of the kinds of powerful information analysis tools normally associated with 'big data'

In the US, self-management has a different meaning as it is supported by its long-standing, rights-based legal tradition of civil liberties, a fact evidenced by the more than 100 year

---

1 Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 5.

2 *Human Rights Act 1998* (UK) , Restatement of the Law, 2nd, Torts 1977 (US) ss 652B-652D; European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8 – Privacy); *Hosking v Runting* [2005] 1 NZLR 1; Canada has 4 province based Privacy Acts.

3 Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) 2564; Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010) 147; New South Wales Law Reform Commission, Report 120: *Invasion of Privacy* (2009).

4 Daniel Solove 'Introduction: Privacy Self-management and the Consent Dilemma (2013) 126 *Harvard Law Review* 1880 ; see also Lior Strahilevitz 'A Social Networks Theory of Privacy' (2004) John M Olin Law and Economics Working Paper no 230.

5 *Victoria Park Racing and Recreational Grounds Co Ltd v Taylor* (1937) 58 CLR 479.

6 *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199.

history of no less than four different privacy torts. Nonetheless, the changes wrought by modern communications networks have caused prominent US thinkers in the area of privacy law to question the effectiveness even of rights-based self-management in providing meaningful privacy protection.[7] Daniel Solove argues that even in the context of a rights-based model in the US, self-management approaches cannot be expected to address the challenges of informed consent for the disclosure of personal information by individual internet and social media users.[8] One compelling issue around consent identified by Solove is the privacy challenge posed by the 'aggregation effect'.[9]

The 'Aggregation Effect'

The average domestic internet user lays down thousands of small, separate and isolated parcels of personal information, whether wittingly or unwittingly, and consent or awareness of where it exists is most often in the form of an opt-out or opt-in checkbox or similar. In isolation, each piece of information disclosed is trivial, and so is the treatment of the consent and awareness issue surrounding it when, for example, commenting, tagging or entering a search term. However, the aggregation effect arises from the ability to piece together those disparate pieces of information into a meaningful whole. Data analysis allows patterns of behaviour or indeed inferences of fact to emerge from user data that is qualitatively very different from the individual bits of personal, but not quite private, information from which they have been composed. What may have appeared to be an unrelated, unconnected and innocuous mass of meaningless bits of information, in fact gives rise, through the process of data analysis, to a major revelation about a medical condition, financial stress, extra-marital affair, political affiliations or other information about which an individual may well have a reasonable expectation of privacy.

the aggregation effect arises from the ability to piece together those disparate pieces of information into a meaningful whole

'Graph Search' and the Domestication of Data Analysis

Powerful data analysis tools are more readily associated with the kind of exotic government surveillance technologies, such as 'XKeyScore', that have recently come to light in relation to the US PRISM scandal.[10] However, the recent announcement of Facebook's 'Graph Search' product suggests that increasingly powerful data analysis tools are quickly becoming available to the average social media user. Facebook openly advertises Graph Search as a powerful search tool allowing users to mine ever deeper and richer seams of data about their friends.[11] The data available goes back to the earliest personal details recorded by users of the social network well before such features existed. Unsurprisingly its announcement has already raised significant privacy concerns and reports about the potential of such tools to cause real harm to unwitting users of the platform.[12]

Networked Liability

The potential for a relatively major privacy breach occurring by stealth is further complicated by the fact that data analysis only reveals, rather than discloses, personal secrets by way of search algorithms or by recognition of emergent patterns of behaviour from information that is already available, albeit in a diffuse form, across a network. Quite aside from any legal or ethical questions about how a particular 'fact' or secret was revealed, the results of a search may then be separately disclosed or publicised by the searcher, thereby potentially further breaching established understandings of privacy and confidence rights.

In the case of aggregation, however, the revealing of secrets has not occurred as a result of the tool, but as a result of the user's input which draws together otherwise unrelated pieces of personal information, all of which have been in fact been disclosed with the individual's full consent and under the guise of pro-active 'self-management' of an individual's privacy settings, and in line with various standardised end-user privacy policies. Such circumstances would presumably raise some difficult legal questions for establishing a cause of action in terms of locating liability, if any, between the social media platform, search tool software developer, potential tortfeasor and injured party. At the same time, even for the diligent social media user set on pro-actively managing their privacy settings, it is clearly becoming more and more difficult to erect a fence high enough to anticipate the privacy challenges posed by rapid change.

Statutory Rights and a Climate of Restraint

This article has explored some of the challenges posed to personal privacy by rapidly advancing information technologies which may be too complex to be met by any one strategy in isolation. Alongside the Privacy Act and self-management strategies for ensuring the privacy of individuals, one advantage of Australian legislatures introducing a statutory cause of action would be the normative effects on the privacy relationship between individuals. Addressing what appear to be legitimate fears and concerns of the public, while at the same time fostering a general 'climate of restraint' in the wider community, may be the most important effect of introducing such a civil cause of action.[13]

The recommendations of the ALRC, NSW and Victorian law reform commissions to introduce a statutory right to privacy

---

7 Solove, above n4.

8 Ibid, 1882.

9 Ibid 1889.

10 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation.

11 'Facebook Graph Search' - https://www.facebook.com/about/graphsearch

12 Juliette Garside, 'Facebook Graph Search Privacy Concerns' (23 Jan 2013) *The Guardian UK,* http://www.theguardian.com/technology/2013/jan/23/facebook-graph-search-privacy-concerns?guni=Article:in%20body%20link.

13 John Burrows, 'Privacy and the Courts' (Address to the Privacy Forum, Wellington, New Zealand, 27 August 2008) <www.privacy.org.nz/assets/Files/PAW/10.-Speaker-Professor-John-Burrows.doc> at 10 November 2009, as quoted in VLRC Report at 147, quoted in http://www.dpmc.gov.au/privacy/causeofaction/docs/issues%20paper_cth_stat_cause_action_serious_invasion_privacy.pdf

in Australia should be understood in terms of a strategy to fill a gap left between self-management and regulation under the Privacy Act.[14] The Australian Government has recognised the importance of statutory recognition of privacy as a human right in Australia in view of its commitment to the ICCPR, a point particularly important given the absence of charter-based federal rights.[15] The fact that the courts have indicated their openness to recognition of a common law right does not mean that the issue should simply be abandoned by the Australian legislature. By all accounts it seems that the groundwork has been well and truly laid, yet Australian legislatures remain reluctant to plug the privacy gap and recognise an individually enforceable right to privacy. In the meantime it seems Australian internet users must continue to self-manage and erect ever higher fences to try and ensure their personal privacy.

Xavier Fijac is a law student at the University of New South Wales.

14 Australian Law Reform Commission 'For Your Information: Australian Privacy Law and Practice (ALRC Report 108);

15 *International Covenant on Civil and Political Rights* (ICCPR) Article 17; Department of the Prime Minister and Cabinet 'Issues Paper – A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' 25.