Protecting Consumer Data is in Everyone's Interests

Xavier Fijac considers consumer and private sector interests in the use of Big Data.

As the involvement of private sector technology companies in the US government's surveillance program continues to be revealed, Australian consumers may have legitimate concerns about who is accessing their personal and confidential business information. Indeed, the business models of technology giants such as Google, Microsoft, Apple and Facebook and the digital presence of many businesses increasingly rely on access to consumers' personal data. The potential for targeted marketing and the myriad other business applications of Big Data potentially make consumer information the modern day 'rivers of gold'[1]. However consumers have a legitimate expectation that businesses will deal ethically with the information they hand over in exchange for services. Consumer concerns over unexpected or unauthorized use of personal data by the state or the private sector therefore potentially has the power to impede innovation and enterprise in the future digital economy. By acting to maintain the trust of the consumer, the commercial sector may protect the mutual interests of big data and the consumer, and thereby ensure that the rivers of data keep flowing.

The potential for targeted marketing and the myriad other business applications of Big Data potentially make consumer information the modern day 'rivers of gold'

There is little doubt that companies such as Google, Apple, Facebook and Microsoft are deeply engaged in a data economy. That economy is based on the exchange of consumers' personal data for products and services and includes social media platforms, business tools and cloud-based email, search and other communications products. However, the Orwellian flipside of this innovation around a seemingly insatiable appetite for more and more data raises what Bruce Schneier recently referred to as the spectre of a 'public private surveillance partnership'.[2]

This 'partnership' refers to the apparent co-operation of large commercial private enterprises with the requests by government security agencies in the US to hand over vast amounts of consumer data obtained under individual privacy agreements. Governments, so the theory goes, find it convenient to allow this corporate enterprise to expand with minimal regulation. Partly it is said, to encourage enterprise and innovation but also as a convenient defacto mode of collection and storage of ever more data on citizen-consumers, which it would otherwise lack the political will to collect directly. Under the guise of national security, the US government, in this case, simply demands or unilaterally obtains unfettered access, at will.[3] Between private technology and government security, the consumer citizen's interests in the privacy and security of their personal information appear to be largely ignored.

For Australian users of cloud-based services such as Google's Gmail or Apple's iCloud the fact that the servers are located in the US means they may be subject to domestic surveillance in that jurisdiction under the provisions of the Foreign Intelligence Surveillance Act (***FISA***) and the Patriot Act[4]. Additionally, there is some evidence of disclosures by Australian companies of Australian consumers' information to US government agencies, which presumably falls within r the national security exceptions in the Privacy Act 1988 (Cth) (the ***Act***).[5] Here it is worth considering whether the average consumer using a cloud-based product such as Gmail or iCloud would consider it a more serious breach of privacy for that information to be shared between corporations in the private sector, who may in fact already have that information by consent, or to be subject of large-scale government initiated disclosures and exposed to the risk of abuse by low-level officers of domestic foreign government security agencies.[6]

The policy of the former Australian government appeared inconsistent on these points. It is also difficult to predict how genuine the new federal government will be about protecting individual privacy.

On the one hand recent major privacy reforms (which the then Opposition agreed to pass) may place a rather heavy burden on the private sector to manage personal information and come into effect in March 2014.[7] The incoming changes to the Privacy Principles make Australian companies directly liable for the actions of offshore business affiliates to whom they have disclosed information whether knowingly or otherwise, and give the Privacy Commissioner substantial power to impose penalties of up to $1.7 million for serious breaches. On the other hand, the depth and breadth of surveillance demonstrated by revelations about the US National Security Agency (***NSA***) suggests a kind of government surveillance that threatens to undermine the thrust of privacy legislation in Australia on a fundamental level. And at the same time the staff and resources available to the Privacy Commissioner appear so limited we may question how serious the government is about making sure

1 Jim Manamara, "As the 'rivers of gold' dry up, what business model will save media?" The Conversation, 29 June, 2012, http://theconversation.com/as-the-rivers-of-gold-dry-up-what-business-model-will-save-media-7956.

2 Bruce Schneier, 'The Public Private Surveillance Partnership' Bloomberg, July 31, 2013, http://www.bloomberg.com/news/print/2013-07-31/the-public-private-surveillance-partnership.html.

3 Glenn Greenwald, 'NSA PRISM Program taps into user data of Apple, Google and others', June 7, 2013, The Guardian, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

4 *Foreign Intelligence Surveillance Act of 1978; Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act Of 2001*

5 Linton Besser, 'Telstra Storing data on behalf of US Government', July 16, 2013, Sydney Morning Herald, http://smh.com.au/it-pro/security-it/telstra-storing-data-on-behalf-of-us-government-20130716-hv0w4.html

6 http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/

7 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth); *Privacy Act 1988* (Cth).

the revised Privacy Principles are given force.[8] In this context it seems as though only the open market drivers of consumer behavior (that is, sending their data elsewhere or even refusing to disclose it altogether) may be an increasingly relevant force in shaping the privacy landscape of the future.

Recent developments in the US suggest that technology companies recognize that the impact of consumer behaviour. A recent report by the Washington D.C based think tank 'The Information Technology and Innovation Foundation' suggests that the revelations of the uses of FISA and the Patriot Act could have a real impact on the competitiveness of US based cloud computing industry. The report estimates that the US currently has a 71% market share of what is projected to be a US $200 billion dollar industry by 2016.[9] The threat of a sudden backlash by consumers and businesses concerned about the security of their data stored in US based cloud-systems seems to already be a reality, with 50% of survey respondents in one study indicating an intention to do business elsewhere, and a 45% increase in business for a Swiss hosting company following the PRISM leaks.[10]

The threat of a sudden backlash by consumers and businesses concerned about the security of their data stored in US based cloud-systems seems to already be a reality

The actions of the email company Lavabit LLC, also illustrates emerging ethical concerns around maintaining the confidence of consumers. Lavabit LLC recently announced it would shut down its entire operation, built-up over 10 years and servicing some 400,000 customers, and move to file court proceedings. It was protesting against what it claimed were unreasonable requests from the NSA to disclose personal data of its users, one of whom was Edward Snowden.[11] Although only a single, and no doubt extreme example, the words of the Lavabit founder may be of some concern to the US market more broadly when he said 'this experience has taught me – don't trust private data to a company with physical ties to the USA'.[12]

The largest players in the corporate technology sector are also showing clear signs of discomfort in being seen to form too close a relationship with government at the expense of the consumer. For example, Microsoft's recent advertising campaign 'Your Privacy is Our Priority' is clearly aimed at addressing consumer confidence head on and attempting to gain market share by appealing to user concerns over privacy.[13]

Furthermore, Yahoo CEO Marissa Mayer and Facebook CEO Mark Zuckerberg have recently stepped up the rhetoric in a campaign to increase transparency around NSA information requests to their companies. Both have publicly criticized what they claim are heavy-handed tactics by security agencies such as the threat of treason for non-compliance by business leaders with their disclosure requests.[14] And both Google and Microsoft recently initiated proceedings in US courts challenging the restrictions on their ability to disclose information about the extent of their compliance with government security and the disclosure of consumer data under FISA.[15] This flurry of very public activity seems to be aimed squarely at maintaining consumer confidence for individual users as well as the business community who may already be using their US cloud-based services anywhere in the world.

Australian consumers are operating in a globally connected and cross-border digital economy. This raises complex challenges for data security and maintaining consumer confidence about who has access to their data. Although there are complex multijurisdictional issues raised by off-shore cloud storage and government and corporate access and control of data stored in cloud systems, it appears that the response of large private sector players is crucial to the future of data security and privacy. Companies who identify and respond to the need to protect their reputation by pro-actively addressing these interests are clearly less likely to suffer the potentially damaging financial and reputational consequences of a consumer backlash. Acting to protect consumer privacy concerns therefore stands to be of ethical and commercial benefit to all and may ensure that consumer data, the modern day 'rivers of gold', will continue to flow in the future.

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

---

8 Peter G Leonard 'Lost in the Privacy Landscape' 06 August, 2013, CIO, http://www.cio.com.au/article/522929/lost_privacy_landscape/

9 Daniel Castro 'How Much Will PRISM Cost the US Cloud Computing Industry?' The Information Technology & Innovation Foundation, August 2013, 1.

10 Ibid, 4.

11 Ladar Levison, Owner of Lavabit LLC, statement available at: http://lavabit.com/.

12 Ibid

13 Frederic Lardinois, 'Microsoft Launches New Online Privacy Awareness Campaign' Tech Crunch, April 22, 2013, http://techcrunch.com/2013/04/22/microsoft-launches-new-online-privacy-awareness-campaign

14 Dominic Rushe, 'Zuckerberg: US government 'blew it' on NSA surveillance – Facebook CEO joins Yahoo's Marissa Mayer in saying the US did 'bad job' of balancing people's privacy and duty to protect', The Guardian, September 12, 2013, http://www.theguardian.com/technology/2013/sep/11/yahoo-ceo-mayer-jail-nsa-surveillance

15 Brad Smith, 'Standing Together for Greater Transparency' Microsoft, 30 Aug, 2013, http://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/08/30/standing-together-for-greater-transparency.aspx: Juha Saarinen 'Microsoft, Google sue US govt over spying disclosure', IT News, Aug 21, 2013