CAMLA COMMUNICATIONS LAW BULLETIN

Communications & Media Law Association Incorporated

Volume 34, No 2. June 2015

Information Privacy and Big Data: Balancing Governance and Business Innovation

Melissa Liu investigates the adequacy of the Australian privacy framework in dealing with challenges arising from Big Data.

INTRODUCTION

In this era, Big Data and privacy protection have become ubiquitous terms. People find themselves scrutinised in nearly all aspects of their lives, with data profiles created from an accumulation of data and a variety of sources predicting but also influencing behaviours. This is particularly the case with the Australian Government recently passing controversial data retention law[1] compelling telephone and Internet security providers to retain users' metadata[2] for two years for security agencies to access in light of increasing terrorism threats.[3] This article addresses the issue of whether the privacy frameworks we have in place sufficiently address Big Data practices, that is, the aggregate collection, sharing and use of data on a large scale crossing jurisdictional boundaries as well as public and private spheres. It has been brought to light that Big Data practices can be useful, such as assisting with business innovation,[4] while at other times, it can be damaging to individuals, governments and organisations. The underlying question is how or whether we can regulate such practices whilst bringing about transparency and accountability.

Given the complexity of this issue, this article will focus only on common Big Data practices and concerns, followed by an analysis of the challenges to the Australian privacy framework (drawing on comparative experiences in the European Union (***EU***) and the United States (***US***)).

>

1 *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

2 Information used to describe other data. See Blake Anthony Klinkner, 'Metadata: What is it? How can it get me into Trouble? What can I do about it?' 31 (2014) *The Wyoming Lawyer* 18.

3 Elise Scott, 'Senate Passes Controversial Metadata Laws', *The Sydney Morning Herald* (Sydney), 27 March 2015.

4 Jonathan Straw, *Why 'Big Data' is a big deal?* (2014) Harvard Magazine <http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal> at 10 October 2014; Thomas Davenport, *Big Data at Work: Dispelling the Myths and Uncovering the Opportunities*, (Harvard Business School Publishing, 1st ed, 2014) 31.

CONTENTS

Information Privacy and Big Data: Balancing Governance and Business Innovation

Net Neutrality – Overseas Experiences and Australia

Profile: Page Henty, General Counsel, RACAT Group

Metadata, Privacy and the Right to Personal Information

Australian Internet Data Collection – Are We Fighting To Protect Privacy Which Is Already Lost?

Why Australia Needs Site-Blocking (CAMLA Young Lawyers Essay Winner)

SAVE THE DATE - CAMLA CUP Thursday 13 August

See inside for a chance to win a copy of Jon Ronson's latest book "So You've Been Publicly Shamed"

Information Privacy and Big Data [CONT'D]

> WHAT IS BIG DATA?

Big Data is best understood as a large collection of data from both traditional and digital sources where the volume and variety of data is beyond 'the ability of typical database software tools to manage, capture, retain and analyse'.[5] The kind of data that is collected usually is a mix between unstructured (unorganised, text-heavy data such as tweets, metadata and social media posts) and multi-structured (such as web log files with a combination of text and visual images). Governments and business organisations engage in new Big Data practices to attain the value and insights from this information, brought about through digital technology and networks.[6]

By tracking and analysing her spending habits Target was able to determine with unsettling accuracy a) she was expecting a baby and b) how far along she was with her pregnancy

Predictive analysis, for instance, through the use of data profiles constructed through surveillance, data collection and aggregation, infringes on an individual's privacy. Perhaps the most dramatic example occurred in early 2012 when Target's predictive analysis of Big Data worked out that a teenage girl was pregnant (before her father knew), but did not flag that she was a teenager, and sent her direct marketing for baby and maternity products.[7] By tracking and analysing her spending habits Target was able to determine with unsettling accuracy a) she was expecting a baby and b) how far along she was with her pregnancy.[8] The current regulation of Big Data practices however is challenging and questionable.

BIG DATA CHALLENGES TO THE CURRENT REGULATORY FRAMEWORK

There is no specific 'Big Data law'. Each country has its own privacy or data protection laws and overarching international guidelines such as the Organisation for Economic Co-operation and Development[9] and the APEC Privacy Framework.[10] The US for example lacks a comprehensive federal law that governs the collection and use of personal data.[11] Instead there is a patchwork of state and federal laws that address particular mediums or industries. These laws cover areas such as credit reporting, electronic communication, videos, call recording and cable communication.[12] In addition, the Federal Trade Commission has the broad authority to pursue companies that engage in unfair or deceptive practices, including inadequate data security measures and failure to comply with privacy policies.[13] The lack of comprehensive federal laws has meant that the US relies on a system of self-regulation through self-imposed privacy policies.[14] The EU, on the other hand, uses an all-inclusive approach with individual privacy rights protected under its Charter of Fundamental Rights[15] and a Data Protection Directive (***Directive***).[16] The Directive restricts the use, sharing, storing, and collecting of personal data. Under the Directive, member states are given flexibility to flesh out the details and, as a result, implementation has varied among countries.

The core issue however is that the underlying principle of privacy regulation and data protection is to protect the data and any records in order to protect an individual's interest.[17] The nature of Big Data, on the other hand, seemingly removes the individual from the collected data, thus removing any justifications for protection under traditional notions of privacy.[18]

AUSTRALIAN CONTEXT

The *Privacy Act 1988* (Cth) (the ***Act)*** in Australia, much like the European Directive, primarily deals with data protection by restricting the collection, use,[19] storage[20] and disclosure of personal information by the public, government or corporations. Arguably one of the strengths of the Act is the fact that it uses 'principles'

5 McKinsey Global Institute, 'Big Data: The Next Frontier for Innovation, Competition, and Productivity' 1 May 2011, 1.
6 Ibid.
7 Kashmir Hill, 'How target figured out a teen girl was pregnant before her father did', Forbes Magazine (online), 16 February 2012; Charles Duhigg, 2012, 'How Companies learn your secrets', *The New York Times*, (online) 16 February 2012.
8 DLA Piper, 'Big Data, Big Issues –Is Australian Privacy Law Keeping Up?' (Research Report, DLA Piper) 26 July 2013.
9 The OECD developed privacy guidelines in 1980, which provided the model for many national privacy laws.
10 APEC Privacy Framework aims to promote a consistent approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows.
11 Herman T. Tervani, *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing* (1st ed, 2010) 166-168.
12 Ibid, 167.
13 Atikus Insurance, 'Big Data's Ethical Dilemma' (Report No 3, Atikus Learning Centre, 19 September 2014) 2.
14 Ibid, 3.
15 *Charter of Fundamental Rights of the European Union* [2012] OJC 326/02.
16 Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
17 Melissa De Zwart, Sal Humphreys and Beatrix Van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37(2) *UNSW Law Journal* 722.
18 Ibid, 722.
19 Australian Privacy Principle 6 –use or disclosure of personal information.
20 Australian Privacy Principle 1 –open and transparent management of personal information.

rather than 'prescriptive rules', which has provided a framework that is 'adequately flexible to respond to technological change'.[21]

Big Data practices challenge these laws by enabling the re-identification of data subjects using non-personal data.[22] Under Australian Privacy Principle (***APP***) 11.3, an APP entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed.[23] It is common practice for governments and business organisations to 'de-identify' or 'anonymise' data prior to conducting analyses or sharing the information with third parties. The dilemma with simply de-identifying information, however, is that with current (and future) technological capabilities, re-identification is more likely to occur when information can be matched or otherwise be tied back to an individual when used in combination with other available information.[24]

Given anonymised data can be typically re-identified, the relevance of regulating personal information under privacy law is restricted. Personal information under the Act is information about an identified or reasonably identifiable individual.[25] Big Data analytics are simply too dynamic and unpredictable to determine if and when particular information or analyses will become or generate personal information.[26] If legislation only regulates personal information, Big Data practices may largely escape regulatory oversight even though it permits inferences of previously private information and the use of group profiling.[27]

Big Data practices also question the need for organisations to provide mandatory notice and obtain consent from an individual before using their information for collection and use.[28] This is to ensure that users make informed decisions about sharing personal information with organisations.[29] While privacy legislation includes other substantive obligations (purpose and use restrictions, security, data quality and access of the data), they have limited impact because they depend on an individual's awareness of their data being processed, the use to which their personal data will be put, and to whom such data will be disclosed.[30] Big Data practices challenge informed choice in three ways:

- Privacy laws apply solely to personal information. But it is not clear whether core privacy principles such as notice and consent apply to newly discovered knowledge derived from personal data, especially when that data has been anonymised or generalised by group profiling.[31]
- Organisations that engage in data collection may find it impossible to provide adequate notice to the individual to make an informed choice, simply because they do not (and cannot) know in advance what they may discover, what insights it may reveal and therefore for what purposes it may be used.[32] The US White House Report stated that notice and consent is defeated by 'exactly the positive benefits that Big Data enables: new, non-obvious, unexpectedly powerful uses of data.'[33] Because future uses would require going back to individuals for their amended consent, many future uses that have significant individual and societal benefits might be simply too costly to undertake.[34]
- It follows that since individuals lack the adequate knowledge of potential correlations and the use of their personal information, they cannot consent knowingly to the use of their data for Big Data analytics.[35] This is particularly the case when individuals are expected to understand and read complicated privacy policies whilst expressing

The current framework clearly leaves an individual's privacy exposed and unduly interferes with the innovation potential of data use

21 Office of the Privacy Commissioner, 'the adequacy of protections for the privacy of Australians online, Submission to Senate Standing Committee on Environment, Communications and the Arts', (*Submission No 16, OPC, August 2010*) 10.

22 Ira S. Rubenstein, 'Big Data: The End of Privacy or a New Beginning?' (Working Paper No 12-56, International Data Privacy Law Advance Access, 25 January 2013) 4.

23 Australian Privacy Principle 11.3 –security of personal information.

24 Department of Finance and Deregulation, 'Big Data –Strategy Issues Paper' (Report, No 12, Commonwealth Government, March 2013) 8.

25 *Privacy Act 1988* (Cth) s6(1).

26 Latanya Sweeney, 'Simple Demographics Often Identify People Uniquely' (Working Paper No 3, Carnegie Mellon University, 2000), 107.

27 Omer Tene and Jules Polonetsky, 'A Theory of Creepy: Technology, Privacy and Shifting Social Norms', (2013) *Yale Journal of Law & Technology*, 66-68, 1717.

28 Fred H. Cate, Peter Cullen & Viktor Mayer-Schonberger, 'Data Protection Principles for the 21st Century Revising the 1980 OECD Guidelines' (Report, Oxford Internet Institute, March 2014) 3-8, Australian Privacy Principle 3 & 5.

29 Fred H. Cate & Viktor Mayer-Schonberger, 'Notice and Consent in a World of Big Data,' (Microsoft Global Privacy Summit Summary Report, November 2012) 3.

30 Above n 91, 5.

31 Group profiling is when profiles are generated and applied to individual members of a reference group, even though a given individual may not actually exhibit the group's properties in question. For instance, the credit or healthcare risks of people living in a certain neighbourhood may be higher than those in other neighbourhoods, which may result in a denial of credit or health insurance coverage for these individuals, even though a specific person living in this neighbourhood pays her bills on time and has a clean bill of health. See Anton Vedder, 'KDD: The Challenge to Individualism' (1999) 1 *Ethics & Information Technology* 275, 277.

32 Henry Davis York, 'Big Data and Analytics: The Power to Transform The Financial Services Industry,' (Report 1 July 2013) 12.

33 Executive Office of the President, 'Big Data and Privacy: A Technological Perspective' (Report, President's Council of Advisors on Science and Technology, May 2014) 4,3.

34 Cate, Cullen & Mayer-Schonberger, above n 30, 4.

> 'informed' consent. Issues with the lack of communication between the individual and the government or business organisation collecting the data, and the inability for the individual to grasp the complexity of the situation would then arise.

RECOMMENDATIONS

The current framework clearly leaves an individual's privacy exposed and unduly interferes with the innovation potential of data use. Perhaps a new perspective of privacy needs to be adopted where the term 'privacy' is another word for information rules. 'Private' does not necessarily mean it is something secretive. Ensuring privacy of data is a matter of defining and enforcing information rules – not just about data collection, but about data use and retention.[36] Further, shared private information can still remain confidential.[37] It is not realistic to think of information in a dichotomy between what is held covert and what is shared, and completely public or completely private. For many reasons, data (and metadata) is shared or generated by design[38] with services involving an individual's trust (eg address books, pictures, GPS, Wifi location which tracks our mobile phones).[39]

Privacy frameworks which aim for transparency should focus on the use of personal information rather than data collection.[40] The context in which personal information will be used and the value it will hold are often unclear at the time of collection.[41] Craig Mundie notes that focusing on the use of personal data does not mean that there should not be responsibilities or regulation relating to data collection, nor should a focus on data collection in specific or sensitive circumstances be abandoned.[42] Rather, in most situations, a more practical balance between Big Data usage and privacy protection is likely to be achieved by focusing on appropriate and accountable use.[43]

Putting greater emphasis on a responsible use framework for organisations shifts the responsibility away from the individual, who often is neither well informed nor well equipped to understand privacy consent notices. It would ameliorate the relative impenetrability of such notices which are currently structured to the advantage of the entities that collect, maintain and use data.[44] Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harm it causes rather than narrowly defining their responsibility to whether they properly obtain consent at the time of collection.[45]

CONCLUSION

Existing privacy frameworks need revision in order to accommodate for the new flow of information and control that Big Data carries in this technological age. Current legislation is overly broad and enables re-identification of information, enabling organisations to link even more information to an individual's profile.[46] This undermines the faith we have in traditional practices for organisations to de-identify raw data sets to protect an individual's privacy. This in turn casts doubt on the fundamental legal distinction between personal data and non-personal data. Further the mandatory notice and consent model underpinning privacy principles is not effective. Privacy notices tend to be convoluted and individuals have become accustomed to pressing 'I agree' without thoroughly understanding or reading the policies. Users therefore cannot knowingly consent.[47]

It should be recognised that privacy is a set of information principles, expanded to include shared information.[48] To mitigate unethical practices, transparency of the Big Data process should be achieved by focusing on the use of personal information rather than data collection.[49] This places more accountability on organisations to create more robust internal compliance and data management programs to ensure appropriate use of the data.

MELISSA LIU is a graduate at Gadens.

35 Rubenstein, above n 22, 4.
36 Neil M Richards & Jonathan H King, 'Big Data Ethics' (2014) 49 *Wake Forest Law Review* 394.
37 Ibid.
38 Many content providers have policies, which encourage and require mutual sharing of data. A two way relationship exists between the organisations (which can be content providers or vendor) and the individual to allow user contributions. See Jacob Harris, 'Messing Around with Metadata', *New York Times* (online), 23 October 2007.
39 Ibid.
40 Cate & Mayer-Schonberger, above n 30; Fred H. Cate, 'The Failure of Fair Information Practice Principles' in *Consumer Protection In The Age Of The Information Economy* (Jane K. Winn (ed.))(Surry, UK: Ashgate 2006); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books (Stanford, California 2010).
41 Cate & Mayer-Schonberger, above n 31, 4.
42 Craig Mundie, 'Privacy Pragmatism: Focus on Data Use, Not Data Collection' (2014) 6 *Council on Foreign Affairs* 3.
43 Ibid, 5.
44 Atikus Insurance, 'Big Data's Ethical Dilemma' (Report No 3, Atikus Learning Centre, 19 September 2014) 2.
45 Executive Office of the President, above n 33, 56.
46 Rubenstein, above n 22, 8.
47 Cate & Mayer-Schonberger, above n 29, 4.
48 Neil M Richards, 'Four Privacy Myths' (2014) 2 *Washington University School of Law* 1, 5.
49 Mundie, above n 42.