EDITORIAL

TRAM NGUYEN[*]

In the aftermath of Edward Snowden's revelations, surveillance practices have been subject to unprecedented public and political debate. Snowden revealed the extent of the National Security Agency's collection and access of communications data, the Five Eyes collaboration, and the cooperation between intelligence agencies and technology companies. Other factors that have likely contributed to this increased scrutiny include the realisation of ubiquitous computing; the shift to storing confidential and personal data on the cloud; and the *News of the World* phone-hacking scandal, which highlighted the commercial availability of surveillance equipment.

Those in favour of mass surveillance assert that such measures are necessary to ensure national security and the prevention of serious crime.[1] In contrast, those against point to the fundamental civil liberties which mass surveillance can undermine, such as the right to privacy,[2] confidentiality, and indirectly, the right to freedom of opinion and expression.[3] The right balance between these competing considerations is controversial. This complexity is well illustrated by the federal government's recent proposal to enact a mandatory data retention regime requiring telecommunication providers to keep customer data records for two years for counter-terrorism purposes.[4] The public backlash[5] and difficulty in defining what would constitute metadata and fall under this regime, illustrate the complexity.

[*] Editor, Issue 37(2), 2014.

[1] See also Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN Doc A/HRC/23/40 (17 April 2013) 3 [3], 4 [12].

[2] Universal Declaration of Human Rights, GA Res 217A (III), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948) art 12.

[3] David Lyon, *Surveillance Studies: An Overview* (Polity Press, 2007) 5.

[4] See Supratim Adhikari, 'Mandatory Data Retention Scheme Inches Closer to Reality', *The Australian* (online), 5 August 2014 <http://www.theaustralian.com.au/business/latest/mandatory-data-retention-scheme-inches-closer-to-reality/story-e6frg90f-1227013855548>; Rosie Lewis, 'ASIO Chief, Malcolm Turnbull, Seek to Reassure Nation over Data Retention Laws', *The Australian* (online), 8 August 2014 <http://www.theaustralian.com.au/national-affairs/asio-chief-malcolm-turnbull-seek-to-reassure-nation-over-data-retention-laws/story-fn59niix-1227017608824>.

[5] See, eg, Ben Grubb, '"Citizens, Not Suspects": GetUp! and Electronic Frontiers Australia Launch Campaign against Mandatory Data Retention', *The Sydney Morning Herald* (online), 12 August 2014 <http://www.smh.com.au/digital-life/digital-life-news/citizens-not-suspects-getup-and-electronic-frontiers-australia-launch-campaign-against-mandatory-data-retention-20140812-1032x4.html>.

A related issue is the use of big data analytics on the data collected from communications surveillance and elsewhere. The phrase 'big data' has attracted much hype and refers to 'the ability of society to harness information in novel ways to produce useful insights or goods and services of significant value'.[6] While this definition highlights the beneficial aspects of the big data phenomenon and makes its application appear innocuous, the use of big data is not without its problems. As the insights are produced by comparing the collected data with other unrelated datasets[7] to reveal hidden behavioural patterns and intentions, this method is equally capable of resulting in discrimination and privacy breaches. Therefore, the challenge with big data will be in balancing its potential against the risks.

The aim of this thematic component has been to build on existing academic literature to elucidate and facilitate discussion of the competing interests in and challenges to communications surveillance and the adoption of big data. The five articles included in this thematic explore topical legal implications surrounding communications surveillance and big data: the use of big data analytics in legal and police decision making and its appropriateness;[8] the challenges to current privacy and anti-discrimination protections posed by big data analytics in employee recruitment and retention;[9] the privacy and democratic implications arising from the public and private sector collecting, retaining and using surveillance data;[10] the challenges to privacy posed by far-reaching state surveillance justified by counter-terrorism rationales;[11] and the applicable legal framework and protections when a citizen discloses classified national security information.[12]

This Issue could not have reached publication without the support and hard work of many generous individuals. First, I would like to express my sincere gratitude to Professor Graham Greenleaf AM, who wrote the insightful Foreword and launched this Issue on 16 September 2014 at Herbert Smith Freehills in Sydney. I would also like to thank Professor David Dixon, the Dean of the University of New South Wales ('UNSW') Faculty of Law for his enthusiasm about this Issue and ongoing support of the Journal. Particular thanks must also

[6] Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt Publishing, 2013) 2.

[7] Lyon, above n 3, 2.

[8] Lyria Bennett Moses and Janet Chan, 'Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools' (2014) 37 *University of New South Wales Law Journal* 643.

[9] Mark Burdon and Paul Harpur, 'Re-conceptualising Privacy and Discrimination in an Age of Talent Analytics' (2014) 37 *University of New South Wales Law Journal* 679.

[10] Melissa de Zwart, Sal Humphreys and Beatrix van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK' (2014) 37 *University of New South Wales Law Journal* 713.

[11] Konrad Lachmayer and Normann Witzleb, 'The Challenge to Privacy from Ever Increasing State Surveillance: A Comparative Perspective' (2014) 37 *University of New South Wales Law Journal* 748.

[12] Keiran Hardy and George Williams, 'Terrorist, Trader, or Whistleblower? Offences and Protections in Australia for Disclosing National Security Information' (2014) 37 *University of New South Wales Law Journal* 784.

go to the Faculty Advisor for this Issue, Professor Michael Handler, for his helpful advice and encouragement.

A great deal of credit belongs to Mr David Vaile, whose guidance was integral to the formulation and development of this theme. It was David who suggested that a thematic issue canvassing the events following the Snowden revelations may be topical and spent many hours explaining the competing interests and tensions to me. Special thanks must also go to Ms Mehera San Roque, Dr Lyria Bennett Moses and Ms Nicola McGarrity, who were very kind in giving their time, leveraging their resources, and entrusting me with their books. I am very grateful for having had the benefit of their considerable expertise and assistance.

I would also like to acknowledge the anonymous peer reviewers whose considered and detailed feedback for each submission to the general and thematic components of this Issue was invaluable. Without their comments, a student-run publication would not have been able to ensure that the best submissions were included or that every submission benefited from constructive feedback regardless of the outcome.

I wish to deeply thank everyone on the Executive Committee and the UNSW Law Journal Editorial Board for their friendship, support and hard work in bringing this Issue to publication. In particular, I am grateful to the 2014 Executive Editor, Guy Baldwin, for his unwavering and thoughtful assistance.

Finally, I thank the authors for their perspicacious and wide-ranging contributions to the topic. It has been an absolute pleasure working on these articles.