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 [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.

Net Neutrality – Overseas Experiences and Australia

Byron Frost tackles the debates surrounding net neutrality in key jurisdictions overseas and the foreseeable implications it could have for Australians.

1. INTRODUCTION

The net neutrality debate is gaining traction around the world, in particular in the United States and Europe, where lawmakers have already taken steps to enshrine the net neutrality principle in law. Meanwhile, net neutrality, the principle that all traffic on the internet should be treated equally, has barely raised an eyebrow in Australia (and is unlikely to) due to the inherent structural differences between the Australian broadband market, and that of the United States.

This paper discusses the net neutrality principle and examines the different approaches taken to regulate the issue in key jurisdictions, namely the United States and Europe. The current and future position in Australia is also considered. At Schedule 1, this paper summarises Foxtel's position in the Australian market and the current over-the-top (***OTT***) players in Australia.

2. WHAT IS NET NEUTRALITY?

Net neutrality is the principle that all traffic on the internet should be treated equally. The term was coined by Columbia University media law Professor Tim Wu when he was discussing the idea that internet service providers (***ISPs***) should be 'common carriers' under US law. 'Common carrier' is a common law term and when applied to the internet, refers to a company that transports content from a content provider to a customer and is responsible for delivery of the goods.[1]

CNET's Marguerite Reardon describes the net neutrality principle as follows:

"whether you're checking Facebook, positing pictures to Instagram, shopping on Amazon, streaming Netflix movies or watching cat videos on YouTube, **all the information traveling across the Internet to you and from you should be treated the same** [emphasis added]".[2]

That is, your ISP, like Telstra's Bigpond or iiNet, cannot block or slow down your access to particular content. In Australia, there are no specific net neutrality laws.

As noted above, the underlying principle of net neutrality is that the internet is open like a public road system as opposed to a toll road system.[3] However whether this principle is commercially practicable is another question altogether that sits at the centre of the debate currently on foot. This is especially the case in the United States, where a new regulatory setting for net neutrality is about to take effect.

3. HOW IS THE NET NEUTRALITY PRINCIPLE DEALT WITH IN KEY JURISDICTIONS?

The net neutrality debate is gaining traction around the world as law makers, ISPs, content producers, distributors and internet users debate on how data flow on the internet should be regulated in the twenty first century. The debate has intensified as the market for content has become more competitive as content has become key to the commercial success of ISPs.

We examine below how key jurisdictions around the world are dealing with the principle of net neutrality.

3.1 United States of America

The loudest debate to date as to whether net neutrality laws should be adopted has been in the United States. This debate came to a head in February 2015 when the Federal Communications Commission (***FCC***) passed new net neutrality rules which classified ISPs under Title II regulation (phone carrier regulations). This new regulatory framework was needed following litigation where the FCC's previous attempts to introduce rules were found to be unlawful, due to the way in which broadband providers were classified by the FCC under US law at the time .

Below, we consider the history of the net neutrality debate in the United States which has led to the current regulatory position.

2010 position

In 2010, the FCC passed rules that forbid the United States' largest cable and DSL ISPs from blocking or slowing online services, while leaving wireless companies with much more latitude to engage in such activity.[4] These rules were known as the *Open Internet Order* and the principle underpinning them was net neutrality.

>

1 Mark Gregory, *NBN and net neutrality: What it means for Australian consumers* (14 November 2014) Business Spectator <http://www.businessspectator.com.au/print/898671> .

2 Marguerite Reardon, *FCC and Net neutrality: What you really need to know* (7 February 2015) CNET <http://www.cnet.com/news/fcc-and-net-neutrality-what-you-really-need-to-know/>.

3 Ibid.

4 Same Gustin, *FCC Passes Compromise Net Neutrality Rules* (21 December 2010) Wired <http://www.wired.com/2010/12/fcc-order/>.

Net Neutrality [CONT'D]

The *Open Internet Order* had three key pillars, as follows:

- **Transparency** – fixed and mobile broadband providers were required to disclose the network management practices, performance characteristics and terms and conditions of their broadband services;
- **No blocking** – fixed broadband providers could not block lawful content, applications, services, or non-harmful devices, and mobile broadband providers could not block lawful websites, or block applications that competed with their voice or video telephony services; and
- **No unreasonable discrimination** – fixed broadband providers could not unreasonably discriminate in transmitting lawful network traffic.[5]

The Court Challenge

The *Open Internet Order* was challenged in federal court by US giant Verizon on several grounds, including that:

- the FCC lacked statutory authority to promulgate the rules;
- the FCC's decision to impose the rules was arbitrary and capricious; and
- the rules contravened statutory provisions prohibiting the FCC from treating broadband providers as common carriers.[6]

On 14 January 2014, the US Court of Appeals for the District of Columbia Circuit:

- affirmed the FCC's authority to regulate broadband internet access service; and
- upheld the FCC's judgment that internet openness encourages broadband investment and that its absence could ultimately inhibit broadband deployment.

Despite these wins for the FCC, the Court only upheld the transparency rule. The no-blocking and no-unreasonable-discrimination rules were invalidated by the Court, because those rules could only apply to common carriers (as defined under US law).[7] The ISPs were not considered common carriers under US law due to a 2005 US Supreme Court decision where the FCC had classified (and the Court had upheld) that cable broadband providers were *integrated information services* and not *telecommunications carriers* subject to Title II regulation (i.e. common carriers) (see *National Cable & Telecommunications Ass'n v. Brand X Internet Services, 545 U.S. 967* (2005)).[8]

The Columbia Circuit Court's decision to vacate two out of the three rules saw the FCC go back to the drawing board to determine how it could legally implement net neutrality rules. The FCC sought public comment on this issue.[9]

A raging debate

How did a seemingly technical set of rules cause such debate within the business and wider community? A number of commentators trace the rise in awareness of net neutrality to a segment by John Oliver on his HBO show *Last Week Tonight*.[10]

In only the show's fifth episode, Oliver launched into a 13-minute piece (the show only runs for about half-an-hour) on the importance of net neutrality. He encouraged his viewers to lodge comments with the FCC on its proposed new rules (this was in June 2014). Oliver said: "Seize your moment, my lovely trolls….turn on caps lock, and fly, my pretties!"

By Monday (the day after the program was broadcast) the FCC's commenting system had stopped working due to the lodgement of more than 45,000 new comments on net neutrality.[11] A principle which Oliver called "even boring by C-SPAN standards"[12] had now grabbed the attention of a large slice of the American population. The FCC eventually received a record 3.7 million comments to its *Notice on Proposed Rulemaking* which began with the fundamental question "What is the right public policy to ensure the Internet remains open?"[13]

5 Federal Communications Commission, *Open Internet Order* (23 December 2010) Federal Communications Commission <https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf>

6 Kevin E McCarthy, *OLR Backgrounder: Appellate Court Decision on Net Neutrality* (11 February 2014) Office of Legislative Research, Connecticut General Assembly <http://www.cga.ct.gov/2014/rpt/pdf/2014-R-0033.pdf>.

7 Ibid.

8 Ibid.

9 *Open Internet* Federal Communications Commission <http://www.fcc.gov/openinternet>.

10 Link to the *net neutrality* segment on HBO's *Last Week Tonight* – www.youtube.com/watch?v=fpbOEoRrHyU

11 Ben Brody, *How John Oliver Transformed the Net Neutrality Debate Once and for All* (27 February 2015) Bloomberg <http://www.bloomberg.com/politics/articles/2015-02-26/how-john-oliver-transformed-the-net-neutrality-debate-once-and-for-all>.

12 Ibid.

13 *Report and Order on Remand, Declaration Ruling, and Order in the matter of Protecting and Promoting the Open Internet* – Federal Communications Commission (26 February 2015) <http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0403/FCC-15-24A1.pdf>, page 23; and Marguerite Reardon, *Net Fix: FCC chief on solving the Open Internet puzzle (Q&A)* 14 January 2015 <http://www.cnet.com/news/net-fix-fcc-chief-on-solving-the-open-internet-puzzle-q-a>.

2015: a dawn of a new era

The FCC's decision to push for new rules was backed by US President Barrack Obama (even though the FCC is an independent government body). The President called an open internet "essential to the American economy, and increasingly to our very way of life."[14]

On 26 February 2015, the FCC passed new rules by three to two Commissioners (the Commissioners voted on party lines) and described the new rules as protecting "free expression and innovation on the Internet" and promoting "investment in the nation's broadband networks."[15]

The new rules, known as 'bright line rules', are guided by the principle that America's broadband networks must be "*fast, fair* and *open*."[16] The rules are as follows:

- **No blocking** – broadband providers may not block access to legal content, applications, services, or non-harmful devices;
- **No throttling** – broadband providers may not impair or degrade lawful internet traffic on the basis of content, applications, services, or non-harmful devices; and
- **No paid prioritisation** – broadband providers may not favour some lawful internet traffic over other lawful traffic in exchange for consideration of any kind – in other words, no "fast lanes".[17]

The new rules also establish that ISPs cannot:

> unreasonably interfere with or unreasonably disadvantage the ability of consumers to select, access, and use the lawful content, applications, services, or devices of their choosing; or of edge providers to make lawful content, applications, services or devices available to consumers.[18]

While the new rules prohibit 'throttling' and 'blocking', they also introduce the concept of *reasonable network management* for ISPs. This exception recognises the need for broadband providers to manage the technical and engineering aspects of their networks.[19] ISPs can rely on this exception where the traffic management steps taken can be characterised as steps primarily used for and tailored to achieve legitimate network management, not a business purpose.[20] The scope of this exception is likely to be an area of contention moving forward.

all the information traveling across the Internet to you and from you should be treated the same

As noted above, the *2010 Open Internet Order* was struck down because of the legal authority the FCC relied on to enact the rules, and not the purpose or effect of the rules. The FCC purported to address this issue in the new rules by reclassifying broadband internet access under Title II of the Communications Act and by relying on section 706 of the Telecommunications Act, i.e. the internet is a telecommunications service. The Court in *Verizon* held that section 706 is an independent grant of authority to the FCC that supports adoption of the *Open Internet Rules*.[21] For those interested in understanding the FCC's legal foundation for the new net neutrality rules, its 400-page order was released publicly on 12 March 2015.[22]

It was widely anticipated that the net neutrality rules would be challenged in the US Courts by ISPs,[23] however challenges could not be brought until the rules "were formally published in the Federal Register, the nation's official record of government actions."[24] Publication occurred on 13 April 2015.[25] The rules will come into effect 60 days after their publication in the Federal Register.[26]

Almost immediately after publication, the USTelecom trade group, National Cable and Telecommunications Association (***NCTA***), CTIA-The Wireless Association and American Cable Association filed petitions in the US Court of Appeals for the D.C. Circuit challenging the validity of the rules. AT&T also filed a petition.[27]

>

14 Brody, above n 11.

15 *FCC Adopts strong, sustainable rules to protect the open internet* (26 February 2015) Federal Communications Commission <http://www.fcc.gov>.

16 Ibid.

17 Ibid.

18 Ibid.

19 Ibid.

20 Ibid.

21 Ibid.

22 *Protecting and Promoting the Open Internet – Report and Order on Remand, Declaratory Ruling, and Order* (12 March 2015) Federal Communications Commission <http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0312/FCC-15-24A1.pdf>.

23 Marguerite Reardon, *13 things you need to know about the FCC's Net neutrality regulation* (14 March 2015) Cnet <http://www.cnet.com/news/13-things-you-need-to-know-about-the-fccs-net-neutrality-regulation/>.

24 Ryan Knutson, FCC Sends Net Neutrality Rules to Federal Register (1 April 2015) Wall Street Journal <http://www.wsj.com/articles/fcc-sends-net-neutrality-rules-to-federal-register-1427927749>.

25 Cat Zakrzewski, *After Net Neutrality Rules Are Published, Congressional Republicans Take A Stand* (13 April 2015) Tech Crunch <http://techcrunch.com/2015/04/13/after-net-neutrality-rules-are-published-congressional-republicans-take-a-stand/?ncid=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Techcrunch+%28TechCrunch%29>.

26 Malathi Nayak, *AT&T, trade groups mount court challenge to FCC Internet rules* (14 April 2015) Reuters <http://uk.reuters.com/article/2015/04/14/uk-fcc-netneutrality-idUKKBN0N51NT20150414>.

27 Ibid.

Net Neutrality [CONT'D]

> According to *The Wall Street Journal* the filings by AT&T, USTelecom, NCTA and CITA are nearly identical, with the rules being challenged on the basis that they are arbitrary and capricious, and violate federal law.[28] Michael Powell, the NCTA's CEO said in a statement that:

> This appeal is not about Net neutrality but the FCC's unnecessary action to apply outdated utility style regulation to the most innovative network in our history…[29]

we see that ISPs were using that technology to influence their own content over other content then that would be of concern to us

It is unclear when these proceedings will be heard. CNET reported that if NCTA and others ask for a stay, a court could block the rules from taking effect if it decides any of the lawsuits have merit.[30]

Response to the new rules

The new *Open Internet Rules* have been approved by the FCC but because they are now subject to legal challenges and because they have not yet taken effect, they have not reached the end of their journey.

Although the White House has endorsed the FCC's decision saying that the new rules "…will protect innovation and create a level playing field for the next generation of entrepreneurs",[31] there has been strong criticism of the FCC's move. Those opposed to the new rules argue that they will stymie rewards for successful innovation[32] and that the legal foundation on which the rules have been developed affords too much power to the FCC. There are also arguments that the onerous compliance costs will have negative economic consequences for ISPs and limit investment in network infrastructure.[33]

The FCC has said that incentives for broadband operators to invest in their networks remain in place, as amongst other things, the new rules forbid the FCC from applying utility-style rate regulation, including rate regulation or tariffs, last-mile unbundling, and burdensome administrative filing requirements or accounting standards.[34] The FCC argues that the rules adopt a 'light-touch' regulatory approach.[35] However, the NCTA, which represents the largest US cable companies, said the new rules:

> …only confirm our fear that the commission has gone well beyond creating enforceable open internet rules, and has instead instituted a regulatory regime change for the internet that will lead to years of litigation, serious collateral consequences for consumers, and ongoing market uncertainty that will slow America's quest to advance broadband deployment and adoption.[36]

Verizon also made view on the FCC's decision clear by releasing a press release in faux typewriter and Morse code formats to emphasise its claim that the FCC had imposed 1930s Rules on the internet. The telecommunications giant said that the:

> …decision by the FCC to encumber broadband Internet services with badly antiquated regulations is a radical step that presages a time of uncertainty for consumers, innovators and investors. Over the past two decades a bipartisan, light-touch policy approach unleashed unprecedented investment and enabled the broadband Internet age consumers now enjoy…the FCC's move is especially regrettable because it is wholly unnecessary. The FCC had targeted tools available to preserve an open Internet, but instead chose to use this order as an excuse to adopt 300-plus pages of broad and open-ended regulatory arcana that will have unintended negative consequences for consumers and various parts of the Internet ecosystem for years to come.[37]

28 Ryan Knutson, AT&T Sues To Overturn FCC's Net Neutrality Rules (14 April 2015) The Wall Street Journal <http://www.wsj.com/articles/at-t-sues-to-overturn-fccs-net-neutrality-rules-1429052166>.

29 Marguerite Reardon, *Cable and wireless industries sue FCC over Net neutrality rules* (14 April 2015) CNET <http://www.cnet.com/news/cable-and-wireless-industries-sue-fcc-over-net-neutrality-rules/>.

30 Ibid.

31 *Net Neutrality: A Free and Open Internet* (26 February 2015) The White House <http://www.whitehouse.gov/net-neutrality>.

32 Brody, above n 11.

33 Geoffrey A. Manne, *Opinion: The FCC's Net Neutrality victory is anything but* (3 March 2015) Wired <http://www.wired.com/2015/03/fcc-better-call-saul/>.

34 *FCC Adopts strong, sustainable rules to protect the open internet* (26 February 2015) Federal Communications Commission <http://www.fcc.gov>.

35 *Report and Order on Remand, Declaration Ruling, and Order in the matter of Protecting and Promoting the Open Internet* – Federal Communications Commission (26 February 2015) <http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0403/FCC-15-24A1.pdf>, page 16.

36 Dominic Rushe, *Critics attack FCC as it releases new rules to protect net neutrality* (13 March 2015) The Guardian <http://www.theguardian.com/technology/2015/mar/12/fcc-rules-internet-report>.

37 *FCC's 'Throwback Thursday' Move Imposes 1930s Rules on the Internet* (26 February 2015) Verizon <http://publicpolicy.verizon.com/assets/docs/VZ_NR_--_2-26-15_VZ_Statement_on_Open_Internet_Order_FINAL_1.pdf>.

America's other major telecommunications provider AT&T joined Verizon in condemning the FCC's decision, stating that:

> unfortunately, the order released today begins a period of uncertainty that will damage broadband investment in the United States. Ultimately, though, we are confident the issue will be resolved by bipartisan action by Congress or a future FCC, or by the courts.[38]

In contrast, Netflix welcomed the FCC's decision as the rules will likely prevent ISPs from throttling Netflix's content streams to customers. Netflix said:

> the net neutrality debate is about who picks winners and losers online: Internet service providers or consumers. Today, the FCC settled it: Consumers win.

Today's order is a meaningful step towards ensuring ISPs cannot shift bad conduct upstream to where they interconnect with content providers like Netflix. Net neutrality rules are only as strong as their weakest link, and it's incumbent on the FCC to ensure these interconnection points aren't used to end-run the principles of an open Internet.

Given the lack of competition among broadband providers, today's other FCC decision preventing regulations that thwart local investment in new broadband infrastructure also is an important step toward ensuring greater consumer choice. These actions kick off a new era that puts the consumer, not litigious corporate giants, at the center of competition policy."[39]

Netflix's position has sparked outrage in some quarters given its deal in Australia with iiNet which exempts Netflix's streams from counting towards an iiNet customer's download cap.[40]

Despite Netflix's position in favour of the rules, its CFO David Wells, in comments at the 2015 Morgan Stanley Technology, Media & Telecom Conference in San Francisco (in March), said the company would have preferred that broadband internet service was not regulated by the US government as a telecommunications utility. However, after some ISPs required payment to deliver video traffic, he was happy with the FCC's recent "Open Internet" ruling.[41] Last year, Netflix cut deals with several big ISPs – including Comcast, AT&T, Verizon and Time Warner Cable – under which it pays for dedicated interconnections. Those deals are to ensure Netflix has enough bandwidth to deliver high-quality streaming video to its subscribers.[42]

In response to the Netflix CFO's comments, Jim Cicconi, AT&T Senior Executive Vice President of External and Legislative Affairs, said:

> Netflix has spun a lot of tales during this FCC proceeding. But it's awfully hard to believe their CFO would go into a major investor conference and misspeak on an issue supposedly so crucial to their future. More likely he had an attack of candor. At least 'til his company's lobbyists got hold of him. I'm sure they'll also have some terrific spin to explain Netflix's data cap deal in Australia.[43]

Since Jim Cicconi made his comments, Netflix has clarified its position on the data cap deals it reached in Australia. In the Q1 2015 Letter to Shareholders, CEO Reed Hastings and CFO David Wells told shareholders that:

> In Australia, we recently sought to protect our new members from data caps by participating in ISP programs that, while common in Australia, effectively condone discrimination among video services (some capped, some not). We should have avoided that and will avoid it going forward.[44]

Therefore the incentive, or at least the need, for ISPs to generally throttle certain traffic is significantly reduced

As such, Netflix is now clearly against data caps as in its view data caps "inhibit Internet innovation and are bad for consumers."[45] Instead, Netflix supports "strong net neutrality across the globe…[as it allows]…all consumers to enjoy the Internet access they pay for without ISPs blocking, throttling, or influencing content in the last mile or at interconnection points."[46]

It's not just carriers and cable companies that object to the new rules, with Finland-based network equipment maker Nokia Networks, whose customers include ISPs, also criticising the new rules. CEO Rajeev Suri said:

> Net neutrality as it exists today needs to change…It will be hard to ensure rock-

>

38 *AT&T Statement on Release of FCC's Net Neutrality Order* (12 March 2015) AT&T Public Policy Blog <http://www.attpublicpolicy.com/fcc/att-statement-on-releaseof-fccs-net-neutrality-order/>.

39 *Netflix says consumers win today's FCC decisions on net neutrality, community broadband* (26 February 2015) Netflix <https://pr.netflix.com/WebClient/getNewsSummary.do?newsId=1941>.

40 Janko Roettgers, *Netflx wont count against iiNet broadband caps in Australia* (2 March 2015) Gigaom <https://gigaom.com/2015/03/02/netflix-wont-count-against-iinet-broadband-caps-in-australia/>.

41 Todd Spangler, *Updated: Netflix CFO Says Pressing FCC for Title II Broadband Regs Was Not Its Preferred Option* (4 March 2015) Variety <http://variety.com/2015/digital/news/netflix-cfo-pleased-with-fcc-title-ii-ruling-although-its-preference-would-have-been-no-broadband-regulation-1201446282/>.

42 Ibid.

43 AT&T Blog Team, *AT&T Remarks on Netflix CFO Remarks* (4 March 2015) AT&T Public Policy Blog <http://www.attpublicpolicy.com/broadband-classification/att-statement-on-netflix-cfo-remarks/>.

44 Reed Hastings and David Wells, *Q1 2015 Shareholder Letter* (15 April 2015) Netflix <http://files.shareholder.com/downloads/NFLX/52537523x0x821407/db785b50-90fe-44da-9f5b-37dbf0dcd0e1/Q1_15_Earnings_Letter_final_tables.pdf>.

45 Ibid.

46 Ibid.

> solid reliability if carriers can't prioritize some network traffic…Yes, it's pro-consumer in the short term, but it won't be pro-consumer in the long term if you don't focus on investment.[47]

Cisco CEO John Chambers told the Mobile World Congress in March 2015 that the US net neutrality rules will help Europe take the lead in broadband because the regulations approved by the FCC will slow down broadband deployment. In his view, the US government should aim for more available broadband instead of focusing on net neutrality.[48]

Dr Hossein Eslambolchi, Chairman & CEO of Cyberflow Analytics wrote on his LinkedIn blog that the net neutrality ruling was analogous to a situation where the Federal Aviation Authority prohibited airlines from offering classes of service.[49]

There is plenty of debate in the US as to whether the net neutrality rules as adopted by the FCC are necessary and the debate is far from over. As noted above, there have already been a number of lawsuits filed seeking that the net neutrality rules be overturned.[50] We will have to wait to see whether the challenges are successful or not.

3.2 Europe

The United States is well-advanced in its net neutrality debate, but what about the other side of the Atlantic?

In March 2014, the European Parliament took its first steps to enshrine the net neutrality principles in law by voting in favour to restrict ISPs from charging data-hungry services for fast network access.[51] The Members of the European Parliament agreed to introduce strict rules to prevent telecoms companies from degrading or blocking internet connections to their competitors' services and applications.[52]

Based on the rules adopted in March 2014, companies would still be able to offer specialised services of higher quality, such as video on demand and business-critical data-intensive cloud applications, provided that it did not interfere with the internet speeds promised to other customers.[53]

In response to the 2014 decision of the European Parliament, four trade bodies representing cable and telecom operators, issued a joint statement noting that:[54]

> Whilst we support an open internet, a set of misconceptions about our industry, together with a rushed legislative process and a lack of technical analysis, risk transforming the Connected Continent Regulation into an anti-innovation and anti-consumer choice legislation.

The proposals will result in a lower quality internet for all. The European Parliament position, as it stands, would put in jeopardy services currently provided to broadband users, such as VPNs for businesses, IP-TV and telepresence. They would also prevent operators from efficiently managing their networks and from providing innovative services that require enhanced levels of quality, such as telemedicine or e-education.

This would threaten innovation and new growth opportunities for those who invest in Europe's digital spine.

A good example is video traffic, which is predicted to rise to 70% of the internet traffic during 2014. Given this impressive figure, the debate around how such traffic is managed and optimized is going to be essential to the effective operation of the internet."[55]

Despite the European Parliament passing net neutrality rules in March 2014, the European Council moved to water them down less than a year later.

This move began in November 2014 under the Italian presidency where the European Council proposed removing the very definition of net neutrality from the rules and allowing differential charging for services.[56] This was followed by the now Latvian-led European

47 Roger Cheng, *Net neutrality critics are flat-out wrong, says FCC chief* (4 March 2015) <http://www.cnet.com/au/news/us-fcc-chairman-net-neutrality-rules-nothing-like-utility-style-regulations/>.

48 Stephen Lawson, *Net neutrality will put U.S. behind Europe, Cisco's Chambers says* (4 March 2015) <http://www.cio.com.au/article/569471/net-neutrality-will-put-u-behind-europe-cisco-chambers-says/>.

49 Dr Hossein Eslamabolchi, *Net Neutrality: One Size Fits All* (5 March 2015) LinkedIn <https://www.linkedin.com/pulse/net-neutrality-one-size-fits-all-dr-hossein-eslambolchi>.

50 Malathi Nayak, *AT&T, trade groups mount court challenge to FCC Internet rules* (14 April 2015) Reuters <http://uk.reuters.com/article/2015/04/14/uk-fcc-netneutrality-idUKKBN0N51NT20150414>.

51 *Net neutrality law adopted by European Parliament* (3 April 2014) BBC News <http://www.bbc.com/news/technology-26865869>.

52 *Net neutrality: Industry MEPs want stricter rules against blocking rival services* (18 March 2013) European Parliament <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fTEXT%2bIM-PRESS%2b20140318IPR39210%2b0%2bDOC%2bXML%2bV0%2f%2fEN&language=EN>.

53 Ibid.

54 *Net neutrality law adopted by European Parliament* (3 April 2014) BBC News <http://www.bbc.com/news/technology-26865869>.

55 *Joint E-Communications Industry Statement on the Open Internet Debate* (1 April 2014) Cable Europe <http://www.cable-europe.eu/joint-e-communications-industry-statement-on-the-open-internet-debate/>.

56 Loek Essers, *Pressure mounts in Europe for strict net neutrality (*27 November 2014) PC World <http://www.pcworld.idg.com.au/article/560573/pressure-mounts-europe-strict-net-neutrality/>.

Council in January this year tabling a compromise text on net neutrality (the European presidency rotates every 6-months).

Under the Latvian proposal, ISPs would be obliged to treat all traffic equally, except where their networks face "congestion", where they were ordered to block some content by a court, or they needed to intervene to ensure the security of the network. ISPs would also be free to offer specialised services, typically at higher speeds and guaranteed quality, as long as broader internet access is not impaired.[57]

In early March 2015, a majority of 28 European Union (***EU***) member states in the European Council voted in favour of changing the rules in line with the Latvian proposal, namely the prioritisation of some "specialised" services that require high quality internet access to function.[58]

The watering down of the proposal sparked opposition from more than 100 members of the European Parliament who in a letter to the Telecoms Council wrote that "weakened proposals on net neutrality go against the European Parliament's repeated calls for clear definitions."[59]

What is the next step in the European debate? The *Financial Times* reported that at the Mobile World Congress in Barcelona in March 2015, the CEOs of both Vodafone and Deutsche Telekom AG (two of Europe's biggest telecommunications companies) argued for rules that would allow them to give priority to specific 'essential' services, like those connected to hospitals or driverless cars.[60]

There is no guarantee that the proposals put forward by Latvia will come into force as drafted. EU lawmaking is a complicated three-way dance between the presidency, the European Parliament and the European Commission, the union's secretariat.[61]

European Commissioner Guenter Oettinger said at the Mobile World Congress in Barcelona (March 2015) that he hopes that the EU will be able to finalise a new law on the subject by the European summer of 2015. The European Commission, as enforcer of the EU's single market, is keen to avoid a situation whereby all 28 states have different rules on regulating internet speeds.[62] At this stage only the Netherlands and Slovenia of the 28-nation bloc have enshrined the net neutrality principle in law.[63]

The Wall Street Journal, reflecting on the recent EU developments, said that:

> Still, this climb down on net neutrality raises the prospect that the EU could end up with a more pro-investment business climate than the U.S. Not everyone wants to follow Washington's lead in tightening government's grip on the Internet.[64]

This pro-business sentiment is reflective of the message from four industry bodies representing the likes of Vodafone, Alcatel-Lucent, Orange and Liberty Global, which said it is "not technologically efficient or beneficial for consumers if all traffic is treated equally. Nor has this ever been the case."[65]

We will have to wait to see what further developments come out of Europe, but at this stage it appears the EU will adopt a less prescriptive regulatory setting (compared to that in the US) as it seeks to protect net neutrality but also develop a single digital economy as a way of driving the European economy forward.

It seems that the rollout of the NBN is not going to result in the principle of net neutrality gaining traction in Australia.

3.3 Australia

Overview

The Australian Communications Consumer Action Network (***ACCAN***) in its submission to the Harper Review noted that Australia has not embraced the ideals of net neutrality to the same degree as the United States.[66] This is because the Australian debate around net neutrality is at a much earlier stage and is heavily influenced by the current market structure for ISPs in Australia.

While some have argued that it is likely that the net neutrality debate in Australia will heat up as the National Broadband Network (***NBN***) becomes the primary medium for content distribution,[67] this author's view is that it is the NBN which in fact will result in the idea of net neutrality never finding strong support in

>

57 Julia Fioretti, *Europe's telecoms heavyweights call for lighter 'net neutrality' rules* (26 January 2015) <http://www.reuters.com/article/2015/01/26/us-eu-telecomunications-neutrality-idUSKBN0KZ21920150126>.
58 Duncan Geere, *Europe reverses course on net neutrality legislation* (6 March 2015) <http://www.wired.co.uk/news/archive/2015-03/06/europe-reverses-on-net-neutrality>.
59 Ibid.
60 Geoffrey Smith, *Net neutrality is not for Europe* (4 March 2015) Fortune <http://fortune.com/2015/03/04/net-neutrality-is-not-for-europe/>.
61 Ibid.
62 Ibid.
63 *Net neutrality law adopted by European Parliament* (3 April 2014) BBC News <http://www.bbc.com/news/technology-26865869>.
64 *Europe's Net Neutrality Sense* (10 March 2015) The Wall Street Journal <http://www.wsj.com/articles/europes-net-neutrality-sense-1426030850>.
65 Julia Fioretti, *Europe's telecoms heavyweights call for lighter 'net neutrality' rules* (26 January 2015) <http://www.reuters.com/article/2015/01/26/us-eu-telecomunications-neutrality-idUSKBN0KZ21920150126>.
66 *Competition Policy Review – Submission by the Australian Communications Consumer Network to the Harper Review* (June 2014) ACCAN <http://competitionpolicyreview.gov.au/files/2014/06/ACCAN.pdf>.
67 Patrick Hubbard, *Bracing the Network for change in 2015* (2 February 2015) ABC Technology and Games <http://www.abc.net.au/technology/articles/2015/02/02/4172375>.

Australia. This view is supported by the limited academic commentary that there is on net neutrality in Australia.[68]

Further, Australia has a powerful competition regulator (the Australian Competition and Consumer Commission (***ACCC***)), which is prepared to intervene where there are attempts to advantage some content over others,[69] therefore negating the need for net neutrality rules. For example, in 2013, Telstra revealed plans to test new ways of managing its broadband network with some of its Victorian customers. The effect of the tests would be to slow-down content for some high-bandwidth internet content.[70] The ACCC Chairman Rod Sims' position on the issue was clear, he said "where traffic management practices are implemented, however, network providers should ensure that such practices are transparent and customers can easily understand the implications of these practices on the service they receive."[71]

Sims told *The Australian Financial Review* that "clearly there is a vertical integration issue where internet service providers can control what comes down their pipe and obviously if, unrelated to reports about Telstra, **we see that ISPs were using that technology to influence their own content over other content then that would be of concern to us** [emphasis added]."[72]

Differences between USA and Australia

One of the key reasons the net neutrality principle is unlikely to be enshrined into law in Australia is that the broadband market in Australia is markedly different to that in the United States both through the payment model adopted and the number of ISP competitors in each market.

User-pay model

The distance between Sydney and Los Angeles is some 12,066 kilometres. Distance is a crucial factor as to why broadband providers in Australia have adopted a user-pays model instead of selling speed (as in the US).

The backbone of the internet is in the United States, which means that Australia's broadband market has developed differently due to the high cost of transmitting data to the internet's backbone.[73] These high costs had to be covered by charges on users related to their downloading, resulting in a user-pay model. In the US, close proximity to the backbone meant that these transmission costs were minimal and the service providers absorbed this cost, resulting in a speed payment model.[74] For example:

- in Australia, iiNet offers a 600GB plan for $69.95 per month on its ADSL2+ network; [75] and
- in the United States, Verizon offers plans of 0.5-1.0 Mbps speed download plans at US$19.99 per month versus enhanced speed plans (up to 7.1-15 Mbps download speeds) at US$29.99 per month.[76]

However with increased hours of video being streamed in the US (Netflix are reportedly responsible for 35% of downstream traffic during peak hours, with YouTube at 14%),[77] broadband providers have sought to develop slow and fast lanes in order to facilitate investment in network infrastructure. On this issue, Jim Cicconi, AT&T's Senior Executive Vice President of External and Legislative Affairs, wrote in an AT&T Public Policy Blog in relation to Netflix that:

> It's simply not fair for Mr. Hastings to demand that ISPs provide him with zero delivery costs – at the high quality he demands – for free. Nor is it fair that other Internet users, who couldn't care less about Netflix, be forced to subsidize the high costs and stresses its service places on all broadband networks.[78]

The position is substantially different in Australia where consumers have now accepted the user-pay model for both fixed and wireless broadband solutions. Therefore the incentive, or at least the need, for ISPs to gen-

68 Angela Daly, *Net Neutrality in Australian: an emerging debate* – Network Neutrality: an Ongoing Regulatory Debate. 2nd Report of the UN IGF Dynamic Coalition on Network Neutrality, (2014), page 48.

69 James Hutchinson, *ACCC takes aim at internet slowdowns* (12 February 2013) The Australian Financial Review <http://www.afr.com/business/telecommunications/accc-takes-aim-at-internet-slowdowns-20130212-j1596>.

70 Ibid.

71 Josh Taylor, *ACCC endorses network congestion pricing* (11 April 2013) ZDNet <http://www.zdnet.com/article/accc-endorses-network-congestion-pricing/>.

72 James Hutchinson, *ACCC takes aim at internet slowdowns* (12 February 2013) The Australian Financial Review <http://www.afr.com/business/telecommunications/accc-takes-aim-at-internet-slowdowns-20130212-j1596>.

73 Gary McLaren, *What the US can learn from Australia on net neutrality* (6 March 2015) Business Spectator <http://www.businessspectator.com.au/article/2015/3/6/technology/what-us-can-learn-australia-net-neutrality>.

74 Ibid.

75 Plan information accessed on iiNet's website on 7 April 2015 - http://www.iinet.net.au/internet/broadband/adsl/.

76 Plan information accessed on Verizon's website on 2 April 2015 – http://www.verizon.com/home/highspeedinternet/.

77 Netflix generates a third of all US web traffic - over twice as much as YouTube (21 November 2014) The Drum <http://www.thedrum.com/news/2014/11/21/netflix-generates-third-all-us-web-traffic-over-twice-much-youtube>.

78 Jim Cicconi, *Who should pay for Netflix* (21 March 2014) AT&T Public Policy Blog <http://www.attpublicpolicy.com/consumers-2/who-should-pay-for-netflix/>.

erally throttle certain traffic is significantly reduced because an ISP can allocate network resources based on the knowledge that it has sold X number of data caps. Further, most data cap plans shape internet speed once the cap is exceeded. This means there is already an accepted throttling practice in Australia as a means for ISPs to manage network traffic.

As such, the need to introduce fast and slow lanes has not arisen and it is unlikely such differentiation will develop so long as a large portion of data is still under the user-pay model, although as discussed later, we note that NBN has introduced the capability for different traffic lanes.[79]

Zero Rating

As noted above, Australian broadband providers sell plans to consumers based on data usage (a user pay model) rather than selling speed. As such, to try and gain a competitive advantage in the market, ISPs have increasingly offered consumers certain services on a zero rating basis when accessed on their network. Zero rating occurs where providers do not charge customers to use data services such as video streaming, that is, use of such services will not 'eat' into the customer's data plans/volume caps.[80]

The practice of zero rating has come to the fore in 2015 with the launch of subscription-video-on-demand (***SVOD***) services and the increase in video content being delivered over IP, such as IPTV. Examples of zero rating options for consumers in Australia, include:

- AFL and NRL mobile streams for Telstra customers record zero data against a customer's cap as Telstra holds the AFL/NRL digital rights;
- Foxtel and Telstra broadband customers can access Presto as unmetered content (Presto is a Foxtel/Seven JV and Foxtel is a News Corp Australia/Telstra company);[81]
- Foxtel from Telstra customers can access Foxtel on-demand content with a zero rating when accessing that content via a Telstra Bigpond account; and
- Netflix can be enjoyed by iiNet customers without impacting a user's iiNet data cap.

While in the US context this practice would likely be frowned upon (especially under the new net neutrality rules), such arrangements do not fall foul of competition laws in Australia.

The future – National Broadband Network

Consumers in Australia understand and accept the practice of ISPs and mobile cellular operators using premium content as a means to grow customer numbers.[82] The question is whether the growth in video content delivered over internet protocol will see ISPs move away from the user-pay model. The rollout of the NBN may influence the strategy of ISPs as it has been built as a tiered service (be that 25Mbs down or 100Mbps down).[83] However, any impact has yet to be seen as current NBN retailers sell plans on a combined speed and data cap usage basis.[84]

More competition would be a better solution

On the issue of speed and data cap plans, *The Australian* recently published comments from Akamai. The global internet infrastructure provider said that it wants to "put an end to the metered internet in Australia" and that it is in discussions with telcos over its plans to do so.[85] Akamai, is reportedly working on turning off metering for some content by making it cheaper for telcos to deliver broadcast quality content across networks.[86]

This move to remove data caps has gained attention recently due to the "Netflix effect" – big increases in internet data use due to an increase in streaming video traffic.[87] There are already reports that iiNet users are suffering slower speeds due to Netflix use on its network since it arrived in Australia in late March.[88]

On the launch of Netflix in Australia, Netflix CEO Reed Hastings said:

> there's no reason for data caps. We want to make the internet unmetered. Period. The capped model is antiquated: we want to make it about speed. 10Mbps will

>

79 Gary McLaren, *What the US can learn from Australia on net neutrality* (6 March 2015) Business Spectator <http://www.businessspectator.com.au/article/2015/3/6/technology/what-us-can-learn-australia-net-neutrality>.

80 Supratim Adhikari, *Netflix takes it on the chin on net neutrality* (5 March 2015) Business Spectator <http://www.businessspectator.com.au/article/2015/3/5/technology/netflix-takes-it-chin-net-neutrality>.

81 Harry Tucker, *How Foxtel Plans to fight Netflix* (23 March 2015) News.com.au <http://www.news.com.au/technology/home-entertainment/how-foxtel-plans-to-fight-netflix/story-fn8tnfhb-1227273967905>.

82 Mark Gregory, *NBN and net neutrality: What it means for Australian consumers* (14 November 2014) Business Spectator <http://www.businessspectator.com.au/article/2014/11/14/technology/nbn-and-net-neutrality-what-it-means-australian-consumers>.

83 Luke Hopewell, Netflix CEO Reed Hastings On The NBN, Piracy And Launching In Australia (24 March 2015) Business Insider <http://www.businessinsider.com.au/netflix-ceo-reed-hastings-on-the-nbn-piracy-and-launching-in-australia-2015-3>.

84 Plan information accessed on iiNet's website on 7 April 2015 - http://www.iinet.net.au/internet/broadband/nbn/plans/.

85 Lara Sinclair, *Netflix effect to pave way for removal of data caps* (6 April 2015) <http://www.theaustralian.com.au/business/media/netflix-effect-to-pave-way-for-removal-of-data-caps/story-fna03wxu-1227292393375>.

86 Ibid.

87 Ibid.

88 Ben Grubb, *The real reason iiNet customers are facing internet speed slowdowns after Netflix's arrival* (8 April 2015) The Age <http://www.theage.com.au/digital-life/digital-life-news/the-real-reason-iinet-customers-are-facing-internet-speed-slowdowns-after-netflixs-arrival-20150408-1mgvas.html>.

> cost more than 1Mbps and 50Mbps will cost more than 10Mbps and that makes sense. Historically, there was so little content in Australia that many users went over the international links and those are pretty expensive, but now there's more and more content and content caching in Australia.[89]

While a charging model based on speed rather than data caps is preferred by services like Netflix as more of their content is likely to be streamed, as Reed Hastings notes the Aussie ISPs "don't really care what we [Netflix] feel." Further, in relation to the net neutrality debate he said that while it is difficult to say whether there will be a fight in Australia over net neutrality, the ISPs are "embracing us [Netflix] because they [the ISPs] get to sell bigger plans…so there's a lot of positives for them in terms of revenue in that way."[90]

Although it is possible that Australia will join the rest of the westernised world in benching data cap plans in favour of selling speed, given that the user-pay model is accepted by consumers (as evidenced by consumers buying higher data caps to facilitate streaming video content) it is unlikely that ISPs will change their position, given that currently it is consumers and not ISPs that effectively cover delivery costs. If this position remains, it is difficult to see a push for specific net neutrality rules gaining traction in Australia and instead competition issues will be left to the ACCC to manage.

NBN Co's product offering features four traffic classes which enables retail providers to develop targeted retail offerings for key segments (e.g. the business market, the voice-only or triple play residential market, etc).[91] This is a form of paid prioritisation which demonstrates that one of the key net neutrality rules has already been thwarted in Australia by commercial realties of a future need for slow and fast lanes. As such, it appears that market forces in a competitive environment will alleviate any net neutrality concerns. The *Business Spectator* notes that:

> …most Australians [currently] experience NBN Co's Traffic Class 4 and this is when traffic is sent across the internet without any quality of service or traffic class management. However traffic class management comes at a cost and Australian RSPs [Retail Service Providers] have been reluctant to embrace the need to provide an improved customer experience.[92]

It seems that the rollout of the NBN is not going to result in the principle of net neutrality gaining traction in Australia. Further data cap plans, where speed throttling is employed by ISPs once a data cap is exceeded (for the remainder of that month's billing period) are an effective means of traffic management for ISPs,[93] meaning there is no incentive for the status quo to change and no desire by consumers for net neutrality to be enshrined in law. For example, Telstra has recently offered (for free) certain data cap increases to its customers, where the cap increase offered was more than double the existing limit.

ISP competition

Aside from the user-pay model and zero rating, the other key difference between the United States and Australia is competition amongst broadband providers.

According to the Australian Communications and Media Authority's (***ACMA***) *2013-14 Communications Report*, there were 71 ISPs with more than 1,000 subscribers operating in Australia as at June 2014, compared to 77 in June 2013. The drop in numbers can be largely attributed to M&A activity. The distribution of ISPs by number of internet subscribers was:

- 45 ISPs with 1,001–10,000 subscribers;
- 18 ISPs with 10,001–100,000 subscribers; and
- eight ISPs with 100,001 or more subscribers.[94]

In 2013 there were 1.2 million people estimated to have switched ISP providers in the previous 12 months.[95] This shows that there is strong competition within the broadband market.

The Australian position is markedly different to that in the United States where a majority of the households are served by only two service providers:

- a cable company; and
- a telecom company.

89 Luke Hopewell, Netflix CEO Reed Hastings On The NBN, Piracy And Launching In Australia (24 March 2015) Business Insider <http://www.businessinsider.com.au/netflix-ceo-reed-hastings-on-the-nbn-piracy-and-launching-in-australia-2015-3>.

90 Ibid.

91 *Ethernet Bitstream Service – Product Fact Sheet* (2014) NBN Co <http://www.nbnco.com.au/content/dam/nbnco2/documents/Ethernet%20Bitsteam%20Fact%20Sheet.PDF>.

92 Mark Gregory, *NBN: The good, the bad and the downright unfair* (16 February 2015) Business Spectator <http://www.businessspectator.com.au/article/2015/2/16/technology/nbn-good-bad-and-downright-unfair>.

93 John de Ridder, *Is this the last chance to reform NBN pricing?* (2 April 2015) CommsWire Magazine, page 25.

94 *2013-14 Communications Report* (December 2014) <http://www.acma.gov.au/~/media/Research%20and%20Reporting/Publication/Comms%20Report%202013%2014/PDF/Communications%20report%20201314_LOW-RES%20FOR%20WEB%20pdf.pdf>.

95 Angela Daly, *Net Neutrality in Australian: an emerging debate* – Network Neutrality: an Ongoing Regulatory Debate. 2nd Report of the UN IGF Dynamic Coalition on Network Neutrality, (2014), pp.43-58, page 48.

Only about 15% have a third option. A quarter of households have one broadband provider or less.[96] Looking at some US states the position is even worse. For example, in Texas, more than 30% of households do not have access to broadband.[97]

The difference between the Australian and the United States market is likely to grow in the coming decade with the rollout of Australia's National Broadband Network (***NBN***) as ISPs become retail providers only by selling access to the NBN, rather than by owning the underlying infrastructure.

The transition has already begun. ACMA found that as at June 2013, 210,628 premises had activated an NBN service, an increase of 200 per cent since June 2012.[98]

As more and more households switch over to the NBN, competition in the retail market will increase, leaving the issue of net neutrality behind. If network speed is being shaped or users are not able to access certain content they will likely just change retail providers. The 1.2 million Australians who changed broadband providers in 2013 evidences a willingness of Australian consumers to preference a better deal over brand loyalty.

Further, as ISPs appear to be adopting a combined speed/data cap plan offering for NBN plans, the need for shaping or blocking content will already have been embedded upfront into the terms of the plan, as choosing a speed/data plan combination is effectively choosing a fast or slow lane to access the internet. This leaves the Australian position markedly different to that in the United States, meaning that for the foreseeable future net neutrality will not be a major factor in Australian broadband policy.

4. CONCLUSION

A recent *Wired* article explained the basis for the net neutrality argument in the American context:

The recent Net neutrality victory at the FCC is not a silver bullet. We can expect costly court challenges, complicated enforcement, and the risks that come with entrusting a large government bureaucracy to manage a technological problem. **More competition would be a better solution** [emphasis added]…As Marc Andreessen recently told The Washington Post, "The ultimate answer would be if you had three or four or five broadband providers to every house."

In such a world, Andreessen explained, "net neutrality is a much less central issue, because if you've got competition, if one of your providers started to screw with you, you'd just switch to another one of your providers."[99]

It is these market and structural differences between the US and Australian broadband markets which result in the net neutrality debate failing to gain traction in Australia. Consumers in Australia already participate in a competitive ISP marketplace with increasing avenues available to access content at good speeds.

As demand for video content grows, Australian ISPs are not needing to make the same capital outlays for infrastructure to meet user demand (as their American cousins) given that the Australian Government (via NBN Co) is building and funding a national broadband network. As such, the net neutrality debate is unlikely to get louder in Australia, especially where competition laws are enforced by a strong competition regulator, the ACCC, which is prepared to intervene where ISP conduct becomes anti-competitive.[100]

NBN Co's Public Affairs Manager Tony Brown wrote on NBN's blog in February that "while the net neutrality drama hasn't yet hit our shores…it does not mean it will not become a major issue here [Australia]."[101] The reasoning for his position was that as the TV market switches from "broadcast-led to broadband-led" some of the US issues may arise here.[102] However this seems unlikely with the broadband market structure that Australia has developed and will continue to develop over the next decade.

Net neutrality is a principle which is being fiercely fought on both sides of the Atlantic. However given Australia's unique differences it is unlikely to follow the path of its northern hemisphere cousins.

BYRON FROST is an Associate in the TMT practice at Allens. The views expressed in this article are the views of the author only and do not represent the views of any organisation.

96 Robert Faris, *Municipal broadband offers hope for lagging US internet* (21 January 2015) The Conversation <http://theconversation.com/municipal-broadband-offers-hope-for-lagging-us-internet-36473>.

97 Masayoshi Son, The Promise of Mobile Internet in Driving American Innovation, the Economy and Education – Transcript of a Presentation by Masayoshi Son (11 March 2014) Softbank Presentation Transcript <http://webcast.softbank.jp/en/press/20140311/pdf/press_20140311_02.pdf>.

98 *2013-14 Communications Report* (December 2014) <http://www.acma.gov.au/~/media/Research%20and%20Reporting/Publication/Comms%20Report%202013%2014/PDF/Communications%20report%20201314_LOW-RES%20FOR%20WEB%20pdf.pdf>.

99 Peter Van Valkenburgh, *Opinion: Bitcoin may be what gets us real net neutrality* (9 March 2015) Wired <http://www.wired.com/2015/03/opinion-bitcoin-may-gets-us-real-net-neutrality/>.

100 James Hutchinson, *ACCC takes aim at internet slowdowns* (12 February 2013) The Australian Financial Review <http://www.afr.com/business/telecommunications/accc-takes-aim-at-internet-slowdowns-20130212-j1596>.

101 Tony Brown, *Net Neutrality – What's the big deal?* (11 February 2015) NBN Co <http://www.nbnco.com.au/blog/net-neutrality-whats-the-big-deal.html>.

102 Ibid.

An Update: Two CAMLA Seminars:

NATIONAL SECURITY: AT WHAT COST?"

Alexandra Morrissey provides an update on the CAMLA's National Security seminar series.

In April and May 2015, CAMLA and the International Institute of Communications (IIC) held a fascinating two part National Security seminar series which explored the way newly enacted national security legislation will impact personal communications, the media and civil liberties in Australia.

SEMINAR ONE "NATIONAL SECURITY: THE NEW LANDSCAPE"

Looked at the political, philosophical and legal framework in which national security legislation has been introduced.

Chaired by Patrick Fair, Partner of Baker & McKenzie, the panel included Dr Daniel Joyce, Faculty of Law, University of NSW and Dr Alana Maurushat, Faculty of Law, University of NSW.

Patrick set the scene by introducing the current features of Australia's national security landscape and summarising security sector reform, cyber security reviews by the Department of Prime Minister and Cabinet, Preventative Detention Orders, data retention laws and laws regarding unauthorised disclosure of 'special intelligence operations'.

He then posed the following questions: "Increased powers for law enforcement and national security have come with provisions that prohibit public reporting and therefore accountability - at what point do these rules go too far? How will we know when they have gone too far?"

Daniel spoke about the importance of free speech, freedom of the press and privacy.

He then asked "should the media be entitled to more freedom and protection? Should journalists be protected as a category, or should public interest disclosures be protected instead? How do we define what a journalist is?"

Finally, he discussed the importance of striking a balance that protects free speech noting that "free speech might be 'delicate' and privacy protection still developing, but both are remarkably resilient rhetorical concepts. Free speech, in particular, facilitates other significant rights and freedoms – it ought to be better protected and valued in our media law and more broadly."

Dr Alana Maurushat brought a fascinating 'insider' perspective to the discussion from a national security standpoint, having worked with security organisations internationally. In relation to the collection and use metadata, Dr Maurushat noted that identification and personal information were not always involved and instead metadata is often used to predict patterns.

Dr Maurushat noted the access to data was important and suggested an automated warrant system should be in place to access data, acknowledging that accessing data without a warrant was problematic but that the standard warrant system would not work in this context.

SEMINAR TWO "NATIONAL SECURITY – WHERE THE RUBBER HITS THE ROAD"

Focused on the practical consequences of the new national security regulatory landscape for journalism, intelligence and law enforcement, telecommunications and personal privacy.

Seminar chair, Dr Daniel Joyce of Faculty of Law, University of NSW, was joined by panellists Georgia-Kate Schubert of Australia's Right to Know Coalition, John Stanton, Chief Executive Officer, Communications Alliance, Professor Barbara McDonald, Faculty of Law, University of Sydney and Bret Walker SC, Barrister, Fifth Floor St James' Hall Chambers.

Georgia-Kate discussed press concerns regarding the new section 35P of the Australian Security Intelligence Organisation Act 1979 (Cth) which deals with the disclosure of information relating to 'special intelligence operations'. In particular she said that there are inadequate protections for whistle blowers and that laws like section 35P allow "source-hunting". This is a major concern for journalists as the ability to report news on matters of public interest is critical.

Bret noted that whistle blower laws and shield laws have to work together; otherwise they make each other redundant.

John then discussed some key concerns relating to the new data retention laws, including the potential for 'scope creep' in relation to both categories of data to be retained and agencies that can gain access to retained data.

As the former ALRC Commissioner for the inquiry into Serious Invasions of Privacy, Barbara McDonald also addressed some key concerns regarding privacy issues raised by the data retention laws, noting there was currently a patchwork of laws relating to privacy with real gaps in privacy protection.

Thanks to CAMLA and IIC and the speakers for making the seminars possible and members and guests for their interesting questions and comments.

ALEXANDRA MORRISSEY is a Lawyer at the Australian Broadcasting Corporation and a member of the CAMLA Young Lawyers Committee.

Profile: Page Henty

General Counsel, RACAT Group and CAMLA President

CAMLA Young Lawyers representative, Hugh Brolsma, caught up with Page Henty (General Counsel at RACAT Group) to discuss her role and anticipated trends and challenges in 2015 and beyond.

1. *Who do you work for?*

I work for the RACAT Group, which no one has ever heard of. It's the holding company for a group of 4 independent TV production houses, mainly producing documentary programs, and a children's subscription television channel.

The production houses are Northern Pictures and Keshet Australia in Sydney, Natural History New Zealand in Dunedin, Washington DC and Beijing, and Beach House Pictures in Singapore.

The children's channel is called *ZooMoo*. It's a new channel (with a synchronised App) for 3 to 6 year olds that focusses on animals. The channel is currently distributed in Asia and throughout Latin America and we expect *ZooMoo* to be available in Australia within the next 6 months.

In total, the Group employs around 300 people worldwide and we're expanding rapidly!

2. *How would you summarise the scope and major responsibilities of your current role?*

I am ultimately responsible for the legal function of all of the RACAT businesses. However, our 4 production houses are largely independent and are managed by experienced and very knowledgeable TV executives with their own legal and administrative teams, who don't usually need day-to-day legal help or support. I get involved in the difficult things that involve more risk than usual, such as difficult co-production or distribution agreements or negotiations for access to sensitive people and places, like the Police or Hospitals where there is a lot of regulation involved.

For the *ZooMoo* channel, I supervise operations and do business development and distribution. My role here is more Business Affairs, and contract negotiation and documentation as part of that.

3. *What prior career path led you to your current role?*

When I started working at what is now Norton Rose in Sydney, pay television was just beginning in Australia and no one understood how the law around it worked! I was really interested in working for media companies and made myself read the then new *Broadcasting Services Act* cover to cover. I didn't remember any of it afterwards but I was lucky enough that it was an environment where I could focus on the television industry and the laws affecting it as a very young lawyer.

That early experience with clients wanting to get into pay TV allowed me to move between law firms in Sydney, Hong Kong and New York doing corporate and commercial, IP and technology work for their media clients. From firms, I went in house for STAR TV in Hong Kong and AUSTAR, Network Ten and now RACAT in Australia.

4. *What do you consider to be some of the interesting and more challenging aspects of your role?*

I am relatively new to the creative side of television, dealing with journalists and producers at the coalface of making sometimes-difficult programs. Last year, for example, Northern Pictures produced a documentary for the ABC called *Changing Minds*, about patients in the secure Mental Health Unit at Liverpool Hospital in Sydney.

The program raised significant legal and ethical issues around consent and privacy which we needed to work through in order to make the program. It was a completely new area for me and I found it fascinating.

That said, the majority of the work I do for RACAT is commercial, ranging from negotiations

to buy satellite capacity to working out tax issues across multiple jurisdictions. The most interesting aspect of the work I do is the diversity, but that is also the most challenging part. When you're working as a lawyer outside a big law firm or company there is rarely an [affordable] expert to turn to, so you need to develop the expertise yourself.

5. *In short, what, in your view, are some of the big issues you are seeing which are currently facing the industry?*

Other lawyers the Bulletin has interviewed for this column have commented on the challenges the television industry is facing with the development of multiple digital distribution platforms for the same content. It used to be that content rights "windows" were well defined and universally accepted. However, what RACAT is seeing, as both a program creator and a channel supplier, is that producers and networks that stick with those old, largely Hollywood-defined rights deals and platforms will be left behind. Both FTA and Pay TV networks worldwide are in the process of working out how to stay relevant and, personally, I don't think TV distributors will be able to survive if they remain just FTA or Pay TV or OTT *etc*. It's interesting watching the programming, corporate and regulatory decisions being made by industry participants to navigate this new digital environment.

Another big issue for me is that with so much free or cheap content available on the Internet, there is a real challenge to make sure really good new content still shines through AND makes enough money to fund the next production. In small markets such as Australia, government policy around local content quotas and production and public broadcaster funding has a huge impact on what programming gets made and broadcast in Australia. Even small regulatory changes in these areas can have a very significant impact from both a cultural and industry perspective. These are areas I watch carefully.

6. *Do you have any hot tips for junior lawyers considering a career in media law?*

Be a good lawyer, first and foremost, in whatever area of practice you are working in whether it is media related or not. Media companies are like any other businesses and need lawyers who know how the law works generally and can do research, negotiate, draft and do all the other boring and fascinating things lawyers do.

When people talk about "media law" I always wonder what they're referring to because there are so many different kinds of media companies and what they do is expanding hugely with the advent of the Internet and digital data and communications.

If I were starting again as a young lawyer, rather than focusing on what kind of media law to practice, I would focus on the kind of company I wanted to work with or to have as my client and try to develop an expertise in the specific media laws that are relevant to its business. Looking at media law from a client's perspective (even a pretend client's perspective) makes the law more relevant and interesting. With a bit of luck, eventually someone will recognise the expertise you've developed and welcome the advice that you can give them.

Oh, and join CAMLA.

HUGH BROLSMA
Senior Associate,
Clayton Utz & CAMLA
Young Lawyers
representative.

IF YOU WOULD LIKE TO SUGGEST SOMEONE TO BE INTERVIEWED BY THE CLB, PLEASE SEND AN EMAIL TO THE EDITORS AT EDITOR@CAMLA.ORG.AU.

Metadata, Privacy and the Right to Personal Information

Tim Brookes, Sophie Dawson and Jessica Norgard explain the recent landmark privacy determination - Ben Grubb and Telstra Corporation Limited – and its impact on how metadata and personal information now can be construed.

BEN GRUBB AND TELSTRA CORPORATION LIMITED [2015] AICMR 35 (1 MAY 2015)

In the lead up to Privacy Awareness Week, the Privacy Commissioner made a landmark determination which helped clarify the Commissioner's view as to what amounts to "personal information". On 1 May 2015, the Privacy Commissioner made a determination that Telstra Corporation Limited (**Telstra**) had breached the *Privacy Act 1988* (Cth) (the **Act**) by failing to provide Mr Grubb with access to some of his personal information, described as "metadata", held by Telstra. The Commissioner found that, in Telstra's hands certain metadata including IP addresses was "personal information" because Telstra could identify individuals by matching the information with information separately held by it in other databases.

Telstra has indicated it will seek review of the decision.

If upheld, the decision will have consequences for the handling of anonymised information which can be matched with other information to identify particular individuals. The decision makes it clear that such information will be treated as Personal Information by the Commissioner even if significant work is required to match information so as to identify individuals.

BACKGROUND

The Act contains a rule which enables individuals to seek access to information about them held by organisations. Until 12 March 2014, that rule was contained in National Privacy Principle 6 (**NPP 6**). From 12 March 2014, NPP 6 has been replaced by Australian Privacy Principle 12 (**APP 12**) which is in similar terms. Relevant parts of NPP 6 and APP 12 are set out below.

On 15 June 2013, Mr Ben Grubb, journalist for Fairfax, sent Telstra a request for "all the metadata information Telstra has stored" about him in relation to his mobile phone service, including cell tower logs, inbound call and text details, duration of data sessions and telephone calls, and the Uniform Resource Locators (**URLs**) of websites visited.

Mr Grubb argued that if Australian law enforcement authorities could request (and gain access to) his personal information, then he should be afforded the same right. The existence of such requests is confirmed in Telstra's Transparency Report (available on Telstra's website) which was taken into account by the Privacy Commissioner, who, in his determination disclosed that Telstra "received and acted on around 85,000 requests for customer information from law enforcement agencies as well as other regulatory bodies and emergency service organisations between 1 July 2013 and 30 June 2014".

Telstra produced a substantial amount of information prior to the Privacy Commissioner's determination. The information produced included call records in relation to all outgoing calls, SMS and MMS messages from Mr Grubb's mobile service, itemised bills to Mr Grubb, subscriber information including name, address, date of birth, mobile number, email address, billing account number, customer ID, IMSI number, PUK, SIM and password information, Mr Grubbs' IMSE, the colour of his mobile phone, his Handset ID, his mobile device payment option, his network type, and 9 to 10 months of call data records in including Mr Grubbs' number, IMEI, IMSI, cell ID, location, original called number, call date, time and duration.

The decision will have consequences for the handling of anonymised information which can be matched with other information to identify particular individuals

Telstra declined to produce certain categories of network data and incoming call records. It submitted that it was not obliged to produce them because:

- In its submission the network data was not "personal information" for the purpose of the Act; and
- Incoming call data was, in its submission, properly characterised as third party personal information disclosure of which would have an unreasonable impact on the privacy of those third parties, and which could contravene relevant *Telecommunications Act 1997* (Cth) provisions.

On 8 August 2013, Mr Grubb lodged a complaint with the Office of the Australian Information Commissioner (the OAIC) under section 36 of the Act, seeking a declaration that Telstra meet its access obligations under the Act.

KEY PRINCIPLES

Under the pre-reform Privacy Act, personal information was defined under section 6 as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably

be ascertained, from the information or opinion" [emphasis added].

This definition was amended as part of the reforms, and is now as follows:

> **Section 6**: ***"personal information"*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.

Section 16 of the pre-reform Act states that an organisation must not do any act that breaches a NPP.

Mr Grubb's request was made under NPP 6, which relevantly provides that: `

> **NPP 6.1**: If an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that (*relevantly here*):
>
> (c) providing access would have an unreasonable impact upon the privacy of other individuals…

Relevant parts of APP 12 are in almost identical terms. They are as follows:

> **APP 12.1**: If an APP entity holds personal information about an individual, that entity must, on request by the individual, give the individual access to the information…
>
> **APP 12.3**: If the APP entity is an organisation then, despite subclause 12.1, the entity is not required to give the individual access to the personal information to the extent that:
>
> (b) giving access would have an unreasonable impact on the privacy of other individuals.

As will be apparent from the consideration below, the Privacy Commissioner's analysis is as relevant to the revised provisions as it is to pre-reform provisions. It is therefore likely that the Privacy Commissioner would reach the same views as those explained below under the amended Act.

DOES METADATA CONSTITUTE PERSONAL INFORMATION?

The question of what constitutes "personal information" is of critical importance to privacy law in Australia, as the Privacy Act only regulates information in this category. It has been the subject of much recent discussion and debate amongst NSW privacy practitioners since the District Court's recent controversial Ritson decision: *R v Ritson; R v Stacey* [2010] NSWDC 160.

Because of the terms in which Mr Grubb's request had been put, the meaning of the term "metadata" was the subject of submissions to the Privacy Commissioner by Telstra and Mr Grubb.

In the end, the Privacy Commissioner's determination was in relation to specific categories of data which Telstra did not provide access to. His decision in relation to each will be briefly summarised in turn.

NETWORK DATA

Telstra identified three sub-types of network data which Mr Grubb had not been provided access to:

- Internet Protocol (IP) address information;
- URL information; and
- Cell tower location information beyond the cell tower location information that Telstra retains for billing purposes (as this had already been provided).

As noted above, the question of whether information is "personal information" under section 6 depends on whether a person's identity is "apparent" or "can reasonably be ascertained" from the information.

APPARENT

Mr Grubb's submissions focussed on his contention that his identity could reasonably be ascertained. He did not argue that it was "apparent" from the data. However, the Commissioner considered this aspect of the test.

The Commissioner accepted the test for "apparent" in *WL v La Trobe University (General)* [2005] VCAT 2592 (**WL**) which was made in relation to a provision in the *Victorian Information Privacy Act* (2000) in identical terms to section 6. That finding was to the effect that a person's identity is only apparent if a person can "look at the information collected and know or perceive plainly and clearly that it was information about the applicant". In WL, Coghlan DP accepted that in some cases a person can be identified by reference to information which is specific to that person other than his or her name or photograph.

The Privacy Commissioner reviewed the metadata in question and considered (in effect by way of obiter) that "the complainant's identity would not necessarily be apparent from some of the metadata he is seeking".

REASONABLY ASCERTAINED

Mr Grubb argued that law enforcement agencies must be able to reasonably ascertain his identity from the metadata to which they obtain access.

The Commissioner accepted Telstra's evidence that network data may, by cross-matching it with other data held on Telstra's various networks and records management systems, link that data to a particular individual.

The Commissioner found on this basis that Mr Grubb's identity could be ascertained. In reaching this conclusion, he had regard to the decision of DP Coghlan in WL that reasonably ascertained "must allow for some

resort to extraneous material" and that "the legislation requires an element of reasonableness about whether a person's identity can be ascertained from material and this will be determined by the circumstances in each case".

Telstra submitted that the metadata retrieval and matching process would be too burdensome in terms of complexity time and cost for the reasonableness criterion to be met. Telstra estimated that the data retrieval and analysis process would take a minimum four days full time engagement for one week's data retrieval or a minimum 12 days full time engagement for four (or more) week's data retrieval. In addition to this Telstra noted that there was a segregation between systems which contain customer records and network data, and that any need to cross-match would have an adverse impact on Telstra's business. While the Commissioner accepted that the process of extracting some of the metadata may be lengthy and require interrogation of databases by specially qualified personnel, when considered in the light of Telstra's resources and operational capacities (and the fact that it already supports this process for information requests from law enforcement bodies), the Commissioner considered that this exercise (and its scope) was reasonable in the circumstances.

Accordingly, the Commissioner determined that the metadata held by Telstra in respect of "network data" constituted Mr Grubb's personal information under the Act, was able to be reasonably ascertained and that this was reasonable under the circumstances, and should be disclosed to Mr Grubb.

INCOMING CALL RECORDS

Telstra identified that incoming call records contain inbound call numbers, location-based information, details of the communication such as time and date and the billing information and subscriber data of incoming callers. Mr Grubb said that his request was limited to the numbers of incoming callers.

As noted above, Telstra argued that this information was not required to be produced for two reasons.

First, Telstra submitted that the information was third party personal information, and not personal information of Mr Grubb.

The Commissioner rejected this argument, and found that an inbound call number, in the context of Mr Grubb's mobile phone activity, comprises shared personal information about Mr Grubb and the incoming caller. The Commissioner also held that while the identity of Mr Grubb would not readily be apparent from the phone number alone, it would be reasonably ascertainable.

Secondly, Telstra argued that it was not obliged to provide access under NPP 6 because providing access would have an unreasonable impact on the privacy of others.

NPP 6.1(a)-(k) provide exceptions to the obligation that an organisation has under the Act to provide an individual with access to their personal information.

As noted above, NPP 6.1(c) provides that an organisation may refuse an individual access to their personal information where the provision of that information would have an "unreasonable impact on the privacy of other individuals".

Referring to the authority of *Smallbone v New South Wales Bar Association* [2011] FCA 1145 [47] the Commissioner noted that whether a disclosure would have unreasonable impact "is a matter of practical judgment having regard of all the circumstances of the case".

The Commissioner considered the different circumstances of incoming calls. For example, if callers take active steps to make their phone numbers silent or blocked, then the Commissioner held that any subsequent disclosure of that information would have an unreasonable impact on the privacy of those callers. Where a caller may have dialled Mr Grubb's number unintentionally, the Commissioner stated that granting subsequent access to the phone numbers of the unintentionally callers would prejudice the privacy of those callers. The Commissioner considered that the position is less certain where a caller intentionally dials Mr Grubb but that it might reasonably be expected that these callers would consent. However, the Commissioner did not draw a firm conclusion on the latter circumstance. The Commissioner also took into consideration Telstra's Privacy Statement and its assurances of confidentiality.

This decision is particularly significant in respect of "anonymised" data, which may constitute personal information, if, when combined with other information, can identify a person.

Telstra indicated that it is possible for specialised staff to interrogate the data for no more than 30 days to identify callers with silent numbers or blocked IDs, however, it is not possible to identify records of persons that unintentionally contacted Mr Grubb.

As it is not possible to edit the records so that only intentional calls are provided, the Commissioner found that Telstra could rely on NPP 6.1(c) to refuse Mr Grubb access.

OUTCOME

The Commissioner determined that Telstra was in breach of NPP 6.1 by failing to provide Mr Grubb with access to the network data above.

The Commissioner held that Telstra must, within 30 business days, provide Mr Grubb with access to his personal information concerning "network data" including IP address

information, URL information and cell tower location information beyond the data already provided. The Commissioner stated that the information should be provided free of charge.

The Commissioner held that Telstra was not required to give access to the phone numbers of incoming callers, and was not in breach of the Act in its refusal to provide this information.

Mr Grubb did not seek an apology or compensation.

LOOKING FORWARD

This decision is particularly significant in respect of "anonymised" data, which may constitute personal information, if, when combined with other information, can identify a person.

This decision also highlighted what the Privacy Commissioner considers to be "reasonable under the circumstances".

Telstra has already indicated that it will be seeking a review of the determination.

The outcome of this review will provide further certainty in this area. This decision and the review hearing will be particularly significant for Carriers and Internet Service Providers affected by the amendments to the *Telecommunications (Interception and Access) Act 1979* (Cth), which requires the retention of metadata for a two-year period.

TIM BROOKES and SOPHIE DAWSON are partners at Ashurst. JESSICA NORGARD is a lawyer at Ashurst.

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

This article considers the impact of proposed changes to the Australian telecommunications data collection regime and suggests that the benefits of the increased data collection and access powers for government intelligence agencies do not justify the intrusion into private lives of individuals.

Editors' note: **The Telecommunications (Intercept and Access) Amendment (Data Retention) Bill 2014 was passed by Parliament without change and received Royal Assent on 13 April 2015. The new Act amends the Telecommunications (Interception and Access) Act 1979 (Cth).**

The past decades have seen the growth and accessibility of affordable technology at all levels of Australian society. The enormous uptake of the internet since its creation in 1969 has meant consumer technologies are more connected than ever before. 'As contemporary life is played out ever more online, the internet has become both ubiquitous and increasingly intimate.'[1] As part of that development the underlying technological platforms are 'not only vulnerable to mass surveillance, they may actually facilitate it.'[2]

As technology costs decrease the potential for mass surveillance continues to broaden throughout the world.[3] Increasingly, 'governmental mass surveillance [is] emerging as a dangerous habit rather than an exceptional measure.'[4]

In Australia, Federal Parliament recently debated *Telecommunications (Interception and Access) Amendment (Data Retention) Bill* 2014 (Cth) (the **Bill**). The Bill proposes changes to the current regime of telecommunications data collection and retention practices by Internet Service Providers (**ISPs**). It seeks to force all ISPs to collect and retain end user data of all users for a two year period in case it is required for criminal law enforcement purposes. [5]

This paper will explore the proposed reforms to the data collection regulatory landscape in Australia and will weigh up the positive and negative aspects of the proposed changes. The activities of intelligence agencies will also be examined, particularly in light of the documents recently leaked by former National Security Agency (**NSA**) analyst Edward Snowden.

The paper concludes that while intelligence agencies may already be privy to more than the proposed telecommunications metadata, that is no reason to accept the increased intrusion into the private lives of citizens by another set of government bodies.

TELECOMMUNICATIONS DATA RETENTION AND ACCESS IN AUSTRALIA NOW

The *Telecommunications (Interception and Access) Act* 1979 (Cth) (the **Act**) governs the interception of, and access to, communications which utilise telecommunications systems.[6] Internet and electronic communications come within the definition of a 'telecommunication network' which itself comprises of connected 'telecommunication systems.' Telecommunications data is within the definition of 'communication' under the Act and includes information about a communication such as phone numbers, email addresses, Internet Protocol (IP) addresses, times, dates and durations of communications. The Act does not prescribe the collection of, retention time or specifics of telecommunication data. That lack of prescription means that providers (including ISPs) determine the type of data collected and length of retention themselves.

In relation to the United Kingdom cases, telecommunications data was able to be used to identify 240 of the suspected 371 offenders.

When one of around 80 prescribed interception agencies wishes to access telecommunications data they are currently required to apply for a warrant from a relevant authority. Without the warrant the interception agency is unable to collect or access stored telecommunications information held by a carrier. To preserve suspected data of evidentiary value

>

1 *The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights,* UN HCHR, 27th sess, [1], UN doc A/HRC/27/37 (2014).
2 Ibid.
3 Ibid [2].
4 Ibid [3].
5 *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Cth) s187A(1) and 187C(1) ('the **Bill**'),
6 Defined by s5(1) of the *Telecommunications (Interception and Access) Act 1979* (Cth).

> an interception agency is also currently able to issue a preservation order on the carrier to ensure retention of the data is maintained where they intend to apply for a stored communications warrant.

Issues arise where, prior to an interception agency requesting a warrant or issuing a preservation order, the carrier (or ISP) destroys, discards or overwrites the stored data. In that case potential probative evidence is forever lost. This issue, which also causes investigations to fail, is the main reason given for the introduction of the Bill to Parliament.[7]

THE PROPOSED SCHEME

The Bill introduced to Parliament in 2014 proposes to rectify the risk of failed investigations due to data being lost before it is secured under a preservation order and warrant. The Bill proposes to:

Prescribe types of telecommunication data by regulation;

Require carriers to retain telecommunication data produced during the provision of telecommunications for two years;

Reduce the number of agencies able to access the data down from more than 80 currently to 'criminal law enforcement agencies' declared by the Minister (likely to be around 20 agencies); and

Broaden the powers of the Commonwealth Ombudsman to inspect and examine records of data collection and interception by criminal law enforcement agencies.

Unsurprisingly, there has been fierce resistance to the amendments from a variety of quarters including privacy advocates, the press, opposition members and the ISP Industry.

THE CASE FOR THE PROPOSED AMENDMENTS

Advocates of the Bill claim a variety of benefits will flow from amending the Act. They also suggest that the amendments are necessary give law enforcement agencies more potency in 'investigating, prosecuting and preventing serious criminal offences (including murder…. kidnapping, drug trafficking…) and activities that threaten national security.'[8]

Government also points out that much of the data is already being collected by ISPs and the Telecommunications Industry and that this data has already been 'kept for long periods and used for billing purposes.

The dynamic allocation of IP addresses by ISPs to customers means that during any given internet session a customer may appear via a different IP address. The use of dynamic IP addresses means that in the majority of cases investigators of criminal conduct need to be able to link an IP address that was in use at a particular point in time 'back to a real world human being.'

The Government pointed to a case where the Australian Federal Police referred child exploitation investigations to both the United Kingdom (which has a data retention law) and to Germany (with no retention laws). In relation to the United Kingdom cases, telecommunications data was able to be used to identify 240 of the suspected 371 offenders. In relation to the German suspects, the authorities, without access to retained telecommunications data, were only able to identify seven out of a possible 377 offenders. Those sorts of figures provide a stark picture of the potential advantages to this type of data retention scheme.

Proponents of the Bill have also tried to maintain that the relevant data being accessed and stored is **not** itself harmful or wrongful content; rather, it identifies the communication. That data, it is argued, is relatively unobtrusive when compared with the actual content.

Finally, the amendments also propose to limit the number of agencies that are able to access the data; down from more than 80 under the current regime to 'criminal law enforcement agencies' which are far fewer in number. That reduction, it is claimed, will 'strengthen privacy protections' for citizens.

Read in isolation, the Government's case sounds sensible and non-controversial. However, to gain a full understanding it is necessary to examine the case against the amendments.

THE CASE AGAINST THE PROPOSED AMENDMENTS

Opponents of the proposed amendments maintain that the 'scheme which requires data to be collected on every customer 'just in case…[it] is needed for law enforcement purposes is *very intrusive* of privacy.''[9] In particular, the Senate Standing Committee raised concerns with the definition of telecommunications data being set by regulation and expected that such a significant matter should appropriately sit with 'Parliament (not the Executive).'[10]

7 Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12560, Malcolm Turnbull, Minister for Communications.
8 Explanatory Memorandum, Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth), 1.
9 Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Alert Digest No. 16 of 2014*, 26 November 2014, 3. (the 'Senate Standing Committee').
10 Ibid above n 36.

The Senate Standing Committee also raised similar concerns with the Minster being empowered to determine the breadth of agencies which qualify as a Criminal Law Enforcement Agency and again suggested that such power was more appropriately allocated to Parliament.[11]

In December 2013, the United Nations General Assembly, of which Australia is a member, reaffirmed the human right to privacy, according to which no one shall be subject to arbitrary...interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference.[12]

The UN considered that 'even the mere possibility of communications information being captured creates an interference with privacy.'[13] One reason for such concern is that 'communications metadata taken as a whole may allow very precise conclusions to be drawn concerning the private lives' of individuals [14]

In fact, the UN Commissioner for Human Rights has pointed out that any breach of privacy must be proportionate to the necessity of the interference and 'actual benefit it yields towards such a purpose.'[15] Most poignantly the UN has said

"Mandatory third-party data retention…where Governments require telephone companies and ISPs to store metadata about their customers' communication and location for subsequent law enforcement and intelligence agency access – appears neither necessary nor proportionate."[16]

The Senate Standing Committee report which included the above passage was produced following the UN General Assembly resolution reaffirming the right to privacy from the exact type of surveillance proposed by the Bill.

The UN's position on collection of telecommunications data is clear and unambiguous and provides great weight to the argument against the proposed regime.

Another argument against the Bill is that there is no requirement or mechanism by which citizens are notified that their data has been collected, accessed or used by criminal law enforcement agencies. The UN notes that such knowledge can help to address interference with or violations of privacy.[17]

Critics of the scheme also claim that use of high grade encryption, virtual private networks (VPN) and email remailers all provide possible ways to avoid parts of the proposed data collection processes.[18] They also claim that criminals and others who are doing wrong using the internet will already be taking steps to avoid data collection, thereby making the scheme intrusive to private citizens for limited benefit.

When considering the pros and cons of the proposed Bill it is, in the author's view, obvious that the risks and possible repercussions for citizen privacy far outweigh the potential benefits of the scheme. The risk of irreparably eroding the reaffirmed universal human right to privacy is unacceptable.[19]

THE INTELLIGENCE ANGLE

Intrinsically linked to data collection of the proposed type is the behaviour of intelligence agencies across the globe, including Australia. As part of the considering the appropriateness of the Bill, it is worth examining some privacy violations that have already been carried out by intelligence services.

Governments including the United Kingdom and United States have argued that monitoring global communications is essential to being able to 'effectively monitor the activities of rogue states, advanced terrorist groups and major organised crime.'

Governments including the United Kingdom and United States have argued that monitoring global communications is essential to being able to 'effectively monitor the activities of rogue states, advanced terrorist groups and major organised crime.'[20] However, of great public interest and concern was the revelation in 2013, by former NSA contractor Edward Snowden, of 'a massive overreach >

11 Ibid, 6.
12 *Resolution on the right to privacy in the digital age*, GA Res 68/167, UN GAOR, 68th sess, 70th plen mtg, UN Doc A/RES/68/167 (2013).
13 *The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights,* UN HCHR, 27th sess, [20], UN doc A/HRC/27/37 (2014).
14 Ibid [19].
15 Ibid [24].
16 Ibid [26].
17 Ibid [40].
18 Talitha Nabbali and Mark Perry, 'Going for the throat: Carnivore in an Echelon World – Part I' (2003) 19 *Computer Law and Society Report* 456, 458.
19 *Resolution on the right to privacy in the digital age*, GA Res 68/167, UN GAOR, 68th sess, 70th plen mtg, UN Doc A/RES/68/167 (2013).
20 *Schrems v Data Protection Commissioner* [2014] 3 C.M.L.R 37, 5.

> on the part of the security authorities, with an almost studied indifference to the privacy interests of ordinary citizens.'[21] The Snowden revelations, which included the release of thousands of classified NSA files, brought to light the activities of the NSA and a range of other intelligence agencies.[22] Those activities included:

Importantly, all is not lost with the proposed scheme. If some of the changes discussed in this paper are ultimately adopted, an acceptable middle ground can be reached.

A program 'code named as PRISM…[which] enables the NSA to collect personal data such as emails, photos and videos from major providers such as Microsoft, Google and Facebook.'[23]

A program entitled "X-Keyscore" [which can] collect "nearly everything a user does on the internet.'[24]

A program which 'allows analysts to search with no prior authorisation through vast databases containing emails, online chats and browsing history of millions of individuals.'[25]

Another large scale communications surveillance system that is in broad use across the globe is the Echelon System. This system is 'a chain of interception facilities located around the world which tap into all the major…international telecommunications networks, including… satellites.'[26] Those facilities are linked together and the 'data they intercept is available to the other participating states.'[27] The United States is the largest participant with other participants including the United Kingdom, Canada, Australia and New Zealand.[28] Local intelligence agencies are mostly prevented from carrying out surveillance on their own citizens, however, some governments have 'through legal loopholes, involving the coordination of surveillance practices…outflanked the protections provided by domestic legal regimes.'[29]

The result of Echelon and other systems used by the intelligence services is that almost every communication across the globe is able to be intercepted and made available. *Put another way, the privacy of every individual worldwide is being breached, routinely and repeatedly by 'mass and largely unsupervised surveillance systems.'*[30]

With that in mind, there is an argument that there is little of our privacy left to protect since our information is already being accessed without our knowledge or consent. It is the author's view that to surrender and open the information gates to an even broader set of agencies risks dangerous future developments that increasingly erode the right to privacy.

IMPROVEMENTS TO THE PROPOSED BILL

Recognising that there is a valid and required change to the data collection and retention practices of the communications industry, there are a number of ways that the regime could be improved. One improvement would be to strike a better balance between the opposing arguments and include the adoption of a range of amendments suggested by Parliamentary Joint Committee on Human Rights in November 2014 which included[31]:

Defining the types of data that will be collected within the legislation and not leaving it to be defined by regulation.[32]

Defining the meaning of 'content' to ensure that the application of the legislation avoids arbitrary interference with privacy.[33]

Reducing the two year retention period to a less lengthy period such as six months, noting the 'low frequency of use of data that is more than six months old.'[34]

Introducing of a minimum severity threshold of the crime being investigated before access to the re-

21 Ibid 8.
22 Ibid 1.
23 Ibid 11.
24 Ibid 12.
25 Ibid.
26 Talitha Nabbali and Mark Perry, 'Going for the throat: Carnivore in an Echelon World – Part II' (2004) 20 *Computer Law and Society Report* 84, 92.
27 Ibid.
28 Ibid.
29 *The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights,* UN HCHR, 27th sess, [30], UN doc A/HRC/27/37 (2014).
30 *Schrems v Data Protection Commissioner* [2014] 3 C.M.L.R 37, 8.
31 Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Fifteenth Report of the 44th Parliament*, (2014).
32 Ibid 1.36.
33 Ibid 1.39.
34 Ibid 1.41.

tained data is granted.[35] The current Bill enables access for any criminal investigation which may lead to large breaches of privacy for relatively trivial offences. One example of such a threshold is the current collection of DNA for arrested persons which can only be collected for categories of serious offences.[36]

Implementing a process where individuals are notified and/or can find out if their data has been accessed.[37]

Implementing a review process where individuals who believe they have had their privacy unnecessarily interfered with can have their matter reviewed by an independent body.[38]

If those amendments were adopted there would be a far greater chance of a system that balanced the proportionality of the invasion of privacy with the likely impact on community safety and the detection and prevention of crime.

CONCLUSION

The *Telecommunications (Interception and Access) Amendment (Data Retention) Bill*[39] proposes a system of data collection that has noble aims. It aims to protect the community from the activities of criminals and terrorists who wish harm on society or to gain benefit illegally.

The acceleration of technologies and their increasing accessibility means that government must act quickly to 'prevent further degradation of the investigative capabilities of Australia's law enforcement and national security agencies.'[40]

Those noble and urgent aims do have a negative side and the proposed system is one that, if implemented will greatly impact the privacy of Australian citizens and residents.

This year the UN has reaffirmed that all people have the right to 'protection against [privacy]…interference or attacks.'[41] Australia, as a member of the UN and a party to the General Assembly, re-affirmed the right to privacy as a basic, fundamental human right.[42] The Australian Government should therefore be cautious in adopting or seeking to adopt a scheme that will almost certainly contradict that right.

Intelligence agencies, including our own, are already party to a broad invasions of our communication privacy. The practices of those agencies have been developing in this field since at least the 1970s[43] and have 'undoubtedly saved many lives and have helped to ensure a high level of security…throughout the…world.'[44] The invasive practices of those agencies appear to be alive and well and realistically are unlikely to change.[45]

The fact that such regular and broad scale privacy incursions already occur is no reason to surrender and allow the gates to our lives to be thrown open to scrutiny by more parts of government. We need to resist the expansion of this sort of behaviour. The Bill should not be allowed to pass in its current form as the price it exacts against privacy is too high.

Importantly, all is not lost with the proposed scheme. If some of the changes discussed in this paper are ultimately adopted, an acceptable middle ground can be reached.

This article was written by a lawyer from Canberra while a student at the University of New England. An earlier version of this article was a finalist in the 2015 CAMLA Young Lawyers essay competition. The views expressed in this article do not represent the interests of any organisation.

---

35 Ibid 1.49.

36 *Criminal Law (Forensic Procedures) Act 2007* (SA), s14(1)(a).

37 Ibid 1.74.

38 Ibid.

39 *2014* (Cth).

40 Commonwealth, *Parliamentary Debates*, House of Representatives, 30 October 2014, 12560, Malcolm Turnbull, Minister for Communications.

41 *The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights,* UN HCHR, 27th sess, [12], UN doc A/HRC/27/37 (2014).

42 *Resolution on the right to privacy in the digital age*, GA Res 68/167, UN GAOR, 68th sess, 70th plen mtg, UN Doc A/RES/68/167 (2013).

43 Talitha Nabbali and Mark Perry, 'Going for the throat: Carnivore in an Echelon World – Part II' (2004) 20 *Computer Law and Society Report* 84, 92.

44 *Schrems v Data Protection Commissioner* [2014] 3 C.M.L.R 37, 5.

45 *The right to privacy in the digital age – Report of the Office of the United Nations High Commissioner for Human Rights,* UN HCHR, 27th sess, [3], UN doc A/HRC/27/37 (2014).

Why Australia Needs Site-Blocking

Sadaat Cheema argues that site-blocking would be an effective and proportionate measure to deal with online copyright infringement in Australia.

INTRODUCTION

With increasing access to high-speed internet and growth in the popularity of file-sharing software (such as BitTorrent), online copyright infringement continues to be a significant issue in many Western countries, Australia included.

Site-blocking does not remove, delete or alter infringing content. It targets the end-user rather than the originator of the content.

On 7 April 2015, the Dallas Buyers Club LLC succeeded in obtaining preliminary discovery of the identification details of approximately 4,726 internet subscribers, suspected of having infringed copyright in the 2012 Jean-Marc Vallee film, *Dallas Buyers Club*. This decision is the first of its kind and opens up the potential for rights-holders to take action against individual internet subscribers. The High Court of Australia has also previously noted, in *Roadshow Films Pty Ltd v iiNet Limited* [2012] HCA 16, that more than half of the usage of iiNet's internet services by customers was attributable to BitTorrent.[1] iiNet is Australia's second largest internet service provider (**ISP**).[2]

At the same time, legislators are turning their attention towards ISPs, as the link between high-speed internet and potential copyright infringement has not gone unnoticed. On 26 March 2015, the Australian Government introduced the *Copyright Infringement (Online Infringement) Bill* (the **Bill**) which amends the *Copyright Act 1968* (Cth) (**Copyright Act**) to enable copyright owners to apply for an injunction requiring ISPs to block access to overseas websites the primary purpose of which is to *'infringe … or facilitate an infringement of copyright'*. In determining whether to grant an injunction, the Court is required to consider a non-exhaustive list of factors including *'whether disabling access to the online location is a proportionate response'*. At the time of writing, the Bill has been presented and read for the first time in the House of Representatives.

The Government's proposal comes in the midst of a polarising debate over the effectiveness, proportionality and due process of a future site-blocking regime. While the entertainment industry regards site-blocking as '*uncontroversial*', the peak telecommunications industry body fears that it could result in unintentional blockage of legitimate websites.[3]

This article argues that site-blocking is, in principle, an effective and proportionate measure to deal with online copyright infringement. It suggests that while some criticisms of siteblocking are valid, they fail to appreciate the nuances of site-blocking, particularly the technical capabilities of the different site-blocking technologies that are available. Having said that, the Government's proposal falls short on important issues. It fails to ensure that a court will give due consideration to selecting a suitable technical measure and the Bill also fails to address a real risk that many applications for site-blocking will go unopposed. These are issues that need to be resolved.

WHAT IS SITE-BLOCKING?

Online copyright infringement can happen in a number of ways: *server-based* models, such as streaming and usenet; *peer-to-peer* networks, such as BitTorrent; and *cloud-based* models such as online locker services. Each model requires that end-users obtain access to a website to begin the download process.

ISPs exercise control over key elements of internet networks which are essential to website accessibility. When a user seeks access to a web page, they rely on a number of internet-related services to transmit data from their computer to the relevant website:

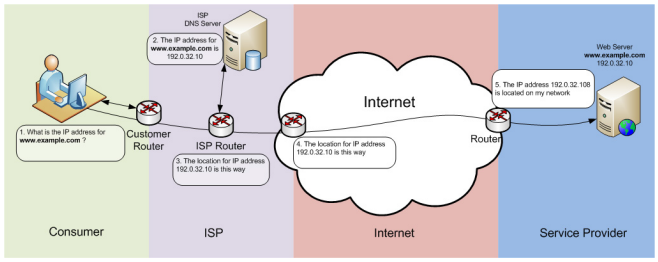
- internet connectivity, as supplied by the ISP;
- Domain Name System (**DNS**) server, which converts a domain name (www.example.com) into an IP address (an IP address is akin to a telephone number; it signifies a particular location (eg of a web server) on the internet);
- network routing, being hardware devices which direct data along the quickest route to an intended destination; and
- web servers, which host websites.[4]

1 *Roadshow Films Pty Ltd v iiNet Limited* [2012] HCA 16 [38].

2 ABC, 'Hollywood studios lose iiNet download case' <http://www.abc.net.au/news/2012-04-20/iinet-wins-download-case/3962442>.

3 Sydney Morning Herald, 'Online pirates hit choppy seas', <http://www.smh.com.au/federal-politics/political-news/online-pirates-hit-choppy-seas-20141212-125ief.html>.

The regulator of communications in the United Kingdom, **Ofcom**, has produced the following diagram to illustrate how data flows along the internet.

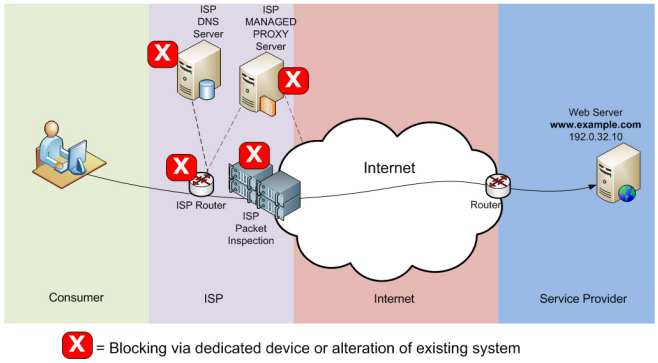


Source: Ofcom.[5]

There are four main technical measures that ISPs can adopt to manipulate the flow of data on the internet and effect a site-block:

- **Blocking by IP Address:** The ISP configures its routers so that data packets that are addressed to an infringing IP address are redirected away from the intended destination.[6]
- **Blocking by DNS:** DNS blocking reconfigures a DNS server so that it refuses to process particular domain names.[7]
- **URL site blocking:** A URL is used to identify a particular file, directory or server. ISPs can use a proxy server to disrupt the flow of data to a particular URL(s).[8]
- **Blocking by Deep Packet Inspection (DPI):** Packet inspection involves the examination of data packets while they are in transit. Data packets which match certain characteristics (eg IP address) are subjected to a reset command, thereby disrupting their flow.

The four technical measures are illustrated in Ofcom's diagram below.



Source: Ofcom.[9]

Site-blocking does not remove, delete or alter infringing content. It targets the end-user rather than the originator of the content. This may be somewhat counterintuitive but it is key to the rationale behind site-blocking.

THE NEED FOR SITE-BLOCKING

Currently, the Copyright Act provides limited scope for rights holders to obtain a site blocking injunction against ISPs. Under section 116AG(3)(a), a court may require an ISP to *'take reasonable steps to disable access to an online location outside Australia'*. The High Court has, however, ruled that this provision is not enlivened where the ISP has not authorised the infringements.[10] So far, no injunction has been granted pursuant to s 116AG(3)(a).[11]

The current legal framework does not, however, provide a no-fault jurisdiction for rights holders to seek site-blocking injunctions. Instead, rights holders are required to bring an action and establish liability of operators of infringing websites. This is impractical for two reasons.

First, it can be difficult to identify the individuals responsible for a particular website. Unfortunately, the registration system for Domain names and IP addresses is not reliable. There is no verification process to confirm identity when an individual registers a domain name or IP address and in some circumstances, individuals can opt-out of providing identification details.[12]

Secondly, website operators and data servers are generally located overseas; service of process and enforcement of judgement can therefore be complex and costly for plaintiffs.

Litigation in the UK against the Newzbin2 website illustrates both of these problems.

Newzbin2 was a website facilitating online copyright infringement via usenet technology. Newzbin2 was based substantially overseas and the operators of the site identified themselves using pseudonyms – *'Mr White'*, *'Mr Black"* and *'Mr Pink'* – and publicly boasted of their success in avoiding enforcement action.[13] Proceedings against Newzbin2 were therefore impractical because the operators could not be identified and their assets were held overseas.

However, the copyright-owners were able to obtain an injunction against an ISP – BT Telecommunications – relying on section 97A of the *Copyright, Designs and Patents Act 1988* (UK).

>

4 Ofcom, '"Site Blocking" to reduce online copyright infringement: A review of sections 17 and 18 of the Digital Economy Act' (2010) 18.
5 Ibid, 19.
6 Above n 4, 28.
7 Ibid, 32.
8 Ibid, 36.
9 Above n 4, 27.
10 Above n 1, [79].
11 Australian Film Bodies, 'Response to Online Copyright Infringement: Discussion Paper' (2014) at 23.
12 Above n 4, 20.
13 *Twentieth Century Fox Film Corporation v Newzbin Limited* [2010] EWHC 608 (Ch), [58].

Why Australia Needs Site-Blocking [CONT'D]

> To date section 97A's no-fault jurisdiction for site-blocking has been used to obtain injunctions in relation to more than 90 websites.[14]

most empirical studies into file-sharing websites have found that less than 5% of their content is legitimate

Given the real difficulties in taking enforcement action against overseas defendants and the limitations of the current legal framework, the rationale for site-blocking is apparent. However, for any site-blocking regime to be successful, it must be effective, proportionate and fair.

ARGUMENTS AGAINST SITE-BLOCKING

The main arguments against the Government's proposal consist of two key points:

- **proportionality:** that site-blocking may result in unintended loss of access to legitimate websites; and
- **effectiveness:** that it is easy to circumvent site-blocking measures.

While these arguments do not justify an outright rejection of the Government's proposal, they do require that certain amendments and clarifications be made.

Proportionality: Over-blocking

A common argument against site-blocking is that it may result in unintended censorship of innocent websites.[15]

"Over-blocking" can occur for two reasons: first, because of the application of an unsuitable site-blocking technique and; secondly, because of the difficulty of ascertaining whether the "*dominant*" purpose of a website is to facilitate copyright infringement.

A frequently cited example of the first reason is s 313(3) of the *Telecommunications Act 1997* (Cth). This section has been used to block websites connected to criminal activity. On one occasion, *ASIC requested that an ISP block access to an IP address, which resulted in the unintended loss of access to thousands of legitimate websites*. Unfortunately, ASIC's personnel were not aware that a single IP address can host multiple websites.[16]

This example should not be seen to suggest that all forms of site-blocking lack precision. As described earlier, there are four main technical measures of site-blocking available and each has a different degree of precision.[17] In the case of ASIC above DNS-blocking may have been more appropriate because this technique targets a particular web domain (eg www.example.com) and would generally not affect unrelated websites.

Initially, the Government's proposal was unclear as to whether the court would need to turn its mind to the most suitable method of site-blocking.[18] However, the Bill now expressly requires the court to consider (amongst other factors) whether the order would be proportionate and the likely impacts. These factors may lead the court to consider the risk of over-blocking but they do not guarantee that this risk will be considered in every case. Accordingly, the Bill should expressly require the court to consider the risk of over-blocking and to select the most appropriate measure of site-blocking.

The second example of overblocking is the evidentiary difficulty of determining whether a website has the '*dominant*' purpose of infringing copyright. According to Levine most empirical studies into file-sharing websites have found that less than 5% of their content is legitimate.[19] This statistic might suggest that most websites which infringe are '*obvious*' cases. However, in the course of any litigation it may be difficult to analyse all of the content on a website, as many file-sharing and file locker websites contain a vast quantity of material. More to the point, there may be real difficulty in proving that the material is unlicensed.

The plaintiffs would of course, be able to lead evidence that media belonging to *them* has not been licensed to the relevant website. However, they would not be in a position to speak on behalf of other rights holders. The concern is made worse by the fact that the Government's proposal contains no mechanism which ensures that an application for a site-blocking injunction is subject to the usual rigours of the adversarial process. Although the Bill requires applicants to notify the site-operator of the application for site-blocking (or at the very least, take reasonable steps to notify) there remains a real risk that many applications may go unopposed as the site operators would be overseas.

In order to address this risk, it is suggested that the Bill should be amended to allow submissions from parties seeking to represent the public interest and from users whose access to the website would be affected. This should make the process more balanced.

14 BBC, 'Blocked piracy site list more than doubles after ruling', <http://www.bbc.com/news/technology-30234790>.

15 iiNet, 'Submission to the Australian Government Discussion Paper: Online Copyright Infringement', (2014) 20.

16 AIMA Digital Policy Group, 'Submission to the Australian Government Discussion Paper: Online Copyright Infringement', (2014) 8.

17 Above n 4.

18 Australian Government, 'Online Copyright Infringement: Discussion Paper' (July 2014) 6.

19 Robert Levine, 'Free Ride: How Digital Parasites are Destroying the Culture Business, and how the Culture Business can Fight Back' (2011) 55.

Effectiveness: Circumvention of Site-blocking

Aside from over-blocking, the other most frequently raised criticism of site-blocking is that it is ineffective. The Pirate Party claims that *'determined users with basic computer literacy will be able to circumvent any blocking mechanism*.'[20]

There are a number of ways that end users can circumvent site-blocking technology, each with a different level of effectiveness. For example, Virtual Private Networks (**VPN**s) cloak the end-user's geographic location by providing an alternative network route for data and enable users to circumvent all of the four major site-blocking methods, even when the methods are used in combination.[21]

Empirical data on the effectiveness of circumvention techniques is conflicting.

Critics of site-blocking point to evidence that despite seizure of The Pirate Bay's servers in Sweden, there was only a small decline in the total number of IP addresses engaged in piracy, which returned to its average level a few days after the raid.[22] This contrasts with the comments of Arnold J in *EMI Records v BskyB* [2013] EWHC (Ch), who referred to evidence that site-blocking measures against The Pirate Bay had caused its site-ranking (a measure of the site's popularity) in the UK to drop from 43rd to 293rd in less than a year.[23]

Two factors make analysing the empirical data difficult: the readiness to circumvent existing laws or technologies and the availability of lawful alternatives, both of which vary from country to country. In some countries, lawful alternatives may be scarce and circumvention strategies well known, making it harder for site-blocking to have great impact. Other countries may lie at the other end of spectrum.

The *inverse* relationship between the convenience of downloading pirated copies and obtaining a lawful copy demonstrates an important point. Site-blocking will make it more difficult to access infringing sites but its effectiveness will depend on other factors, including the rightholders' willingness to ensure their content is conveniently available to consumers. Lawmakers should ensure that consideration is given to other measures directed at educating and deterring consumers such as a graduated response scheme.

What is clear, however, is that site-blocking does cause inconvenience to end users, whether by having to download encryption software or by having to pay a monthly subscription fee for a VPN service. While site-blocking will not keep out the most determined users, it will almost certainly have an impact on others.

CONCLUSION

The international and anonymous nature of copyright infringement means that there are significant difficulties in taking direct enforcement action against website operators. Site-blocking targets end user access within Australia and is therefore a practical alternative option.

At the same time, the Government's proposal should permit standing for those whose interests are affected (ie end users) or who oppose the injunction on public interest grounds. Currently, the Bill confines standing to the rightholder, the ISP and the site-operator. These modifications will ensure that opposing views are heard. The court should also be required to turn its mind to the method of implementation so that the most effective and least disruptive option is pursued.

Site-blocking is not a panacea but it *will* make a significant difference.

SADAAT CHEEMA is a junior lawyer in the Workplace Relations, Employment and Safety team at Clayton Utz. This paper won the CAMLA Young Lawyers Essay Competition in 2015. The opinions expressed in this paper are the views of the author only and do not represent any organisation.

---

20 Pirate Party Australia, 'Submission to the Attorney-General's Department on the Online Copyright Infringement Discussion Paper' (2014) 3.

21 Above n 4, 41.

22 Variety, 'Pirate Bay Shutdown Has Had Virtually No Effect on Digital Piracy Levels', 13 December 2014 <http://variety.com/2014/digital/news/pirate-bay-shutdown-has-had-virtually-no-effect-on-digital-piracy-levels-1201378756/>.

23 *EMI Records v BskyB* [2013] EWHC (Ch) [106].

CONTRIBUTIONS & COMMENTS

Contibutions and Comments are sought from the members and non-members of CAMLA, including features, articles, and case notes. Suggestions and comments on the content and format of the Communications Law Bulletin are also welcomed.

Contributions in electronic format and comments should be forwarded to the editors of the Communications Law Bulletin at editor@camla.org.au or to

Valeska Bloch or Victoria Wark

C/- Allens
Deutsche Bank Place
Corner Hunter & Philip Streets
SYDNEY NSW 2000

Tel: +612 9230 4000
Fax: +612 9230 5333

CAMLA contact details:

Email: camla@tpg.com.au
Phone: 02 42 948 059
Mail: PO Box 237,
KINGSFORD NSW 2032

About CAMLA

The Communications and Media Law Association Incorporated (CAMLA) brings together a wide range of people interested in law and policy relating to communications and the media. CAMLA includes lawyers, journalists, broadcasters, members of the telecommunications industry, politicians, publishers, academics and public servants. Issues of interest to CAMLA members include:

- defamation
- broadcasting
- copyright
- advertising
- information technology
- freedom of information
- contempt
- privacy
- censorship
- film law
- telecommunications
- the Internet & online services

In order to debate and discuss these issues CAMLA organises a range of seminars and lunches featuring speakers prominent in communications and media law policy.

Speakers have included Ministers, Attorneys-General, members and staff of communications regulatory authorities, senior public servants, executives in the communications industry, lawyers specialising in media and communications law, and overseas experts.

CAMLA provides a useful way to establish informal contacts with other people working in the business of communications and media. It is strongly independent, and includes people with diverse political and professional connections. To join CAMLA, or to subscribe to the Communications Law Bulletin, complete the form below and forward it to CAMLA.

Disclaimer

The Communications Law Bulletin is the journal of the Communications and Media Law Association which is an independent organisation which acts as a forum for debate and discussion and welcomes the widest range of views. The views expressed in the Communications Law Bulletin and at CAMLA functions are personal views of the respective authors or speakers. They are not intended to be relied upon as, or to take the place of, legal advice.

For further information:

Visit the CAMLA website at www.camla.org.au for information about CAMLA, CAMLA seminars and events, competitions and the Communications Law Bulletin.

To: The Secretary, camla@tpg.com.au or CAMLA, Box 237, KINGSFORD NSW 2032
Phone: 02 42 948 059

Name:

Address:

Telephone: **Fax:**

Email:

Principal areas of interest:

I hereby apply for the category of membership ticked below, which includes a Communications Law Bulletin subscription, and enclose a cheque in favour of CAMLA for the annual fee indicated:

☐ Ordinary membership $130.00 (includes GST)

☐ Corporate membership $525.00 (includes GST)
(include a list of names of individuals - maximum 5)

☐ Student membership $45.00 (includes GST)
(include undergraduate full time student card copy)

☐ Subscription without membership $150.00
(includes GST) (Library subscribers may obtain extra copies for $10.00 each + GST and handling)