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).