Submission to Parliamentary Joint Committee on Intelligence and Security Inquiry into the *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*

Chris Berg
Senior Fellow

January, 2015

Institute of Public Affairs
THE VOICE FOR FREEDOM
ESTABLISHED–1943

www.ipa.org.au

Introduction

Recent terrorist attacks have emphasised the need for counter-terrorism and law enforcement policy to be flexible, robust, and up-to-date. The rise of Islamic State is a significant threat, materially changing the foreign fighter problem. Many of the government's recent anti-terror law changes have been welcome and necessary. As I argued in December 2014, the "knee-jerk reaction against any and all national security changes is not merely wrong, it's dangerous. There is no more basic responsibility of government than security."[1]

However, The *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* ("data retention bill") will mandate the creation of large databases of information about the activities of all Australian internet users, not just those suspected of criminal activity.

The information contained in these databases will be sufficient to reconstruct extremely deep profiles of the activities of internet users. The information within the databases will be potentially available in any court proceeding, including, for instance, as the result of a subpoena in civil litigation. The government has made a decision not to limit access to this information to national security purposes. The creation of these databases manifests substantial new privacy risks to Australians, both from lawful and unlawful access.

The government has not demonstrated that the risks and consequences of mandatory data retention outweigh the benefits to law enforcement, nor has it demonstrated that the existing legal framework – which was substantially revised in 2012 – is insufficient to tackle the security challenges which the government has identified.

[1] C Berg, 'Anti-Terrorism Law Reform Follows Legislate In Haste, Repeal At Leisure Approach', *The Sunday Age,* 7 December 2014. Available at http://www.theage.com.au/comment/antiterrorism-law-reform-follows-legislate-in-haste-repeal-at-leisure-approach-20141206-11zz4h.html.

Why mandatory data retention?

Legislation ought to evolve with changing circumstances. Technological changes (and the changes in social practice which the technological changes have brought about) necessitate changes in government activity and law enforcement. The *Telecommunications (Interception and Access) Act 1979* was itself introduced in recognition of technological change that made the narrow focus in *Telephonic Communications (Interception) Act 1960* on interception by telephone redundant.

The original intent of the 1960 Act was to protect privacy rather than violate it. The Act spelled out a broad prohibition on telecommunications interception and offered only a few small, narrow exceptions, including one which allowed for interception with a warrant for national security purposes but not general law enforcement purposes.[2]

This original intent remains in the Act as it reads in 2015, which is based on the principle that telecommunications interception is unlawful unless it meets one of the exceptions. However the exceptions have broadened out considerably, allowing for three separate telecommunications interception and access regimes.

The first allows for real-time interception by the Australian Security Intelligence Organisation and other law enforcement agencies. The second allows for access to stored communications that may be held by telecommunications carriers. Both of these two regimes require warrants for lawful access.

The third regime allows for warrantless access by law enforcement and other revenue raising agencies to telecommunications *data* – commonly known in the public debate as "metadata". The idea behind this lower threshold for access is that the information is lesser than full "content" data such as the actual text of an email. It has been widely suggested that therefore metadata access is less intrusive of privacy.

This is an unfortunate misconception of the significance of metadata. Metadata is not less intrusive than content data. Metadata is valuable to law enforcement agencies because it provides a more comprehensive account of the activities of a person of interest than, for instance, a telephone intercept might be. Two characteristics of metadata account for this. First, metadata is machine readable. Where the human speech that might be acquired over a telephone intercept will be full of the complexities and ambiguities of verbal interaction – and require extensive deciphering to be useable – metadata can be inputted into computers to map out a person's activities and communications rapidly. The second is that metadata is collected and used in bulk.

These two features also help to understand the privacy implications of metadata collection. It is not obvious that there is any difference in the degree to which the interception of content data and metadata violates privacy. Parliament should not proceed with the data retention legislation under an assumption that metadata collection is less privacy-intrusive than direct surveillance. In many ways, it can be more-so, as it creates a larger, more comprehensive, and more legible account of a person's private activities.

---

[2] S Rodrick, 'Accessing Telecommunications Data for National Security and Law Enforcement Purposes', *Federal Law Review*, vol. 37, no. 3, 2009.

The telecommunications interception regime has been frequently and steadily expanded in recent decades. Contrary to the assertions of many supporters of data retention, the regime has been constantly "modernised". Since 2001 it has been amended 48 separate times. It is, indeed, this constant modernisation which has led to the complex series of interception regimes, which are now one of the exhibits for the future reform. The 2012 Attorney Generals' Department paper 'Equipping Australia against Emerging and Evolving Threats' emphasised the need for a holistic rethink of the entire surveillance regime to make it internally consistent.[3] This legislation, however, does not achieve that end. Rather it proposes to add an even more complex regulatory burden on the telecommunications sector in order to expand the access regime.

The existing telecommunications data access regime takes advantage of a practice that telephone providers utilise for business purposes – the recording of data about the time, length, and parties to an individual telephone call. This information is retained in order to accurately bill customers, as telephone services are billed typically on a per-call basis or some variation of that system. From this data large amounts of information can be gleaned, but it is important to note that the data exists independently of its law enforcement uses. The data has been created by telecommunications providers for specific business purposes.

In the internet era, this sort of data is both less important and less accessible. Communication that was once done by phone might be done over email, or in a chat room. Telephone calls which were logged on a per-call basis might be conducted over purely internet telephonic services like Skype. Rather than selling customers per-call access, now telecommunications is sold in large blocks of data. The only information needed for billing purposes with internet access might be download volumes. Even then that might not be necessary, either in the case of unlimited download plans or simply because excess downloads are "shaped" – that is, offered freely at a reduced speed – rather than charged back to the customer.

It is true that telecommunications providers keep large amounts of data for a wide range of purposes, and for a highly variable period of time. However, under Australia's privacy principles, which only came in force in its current form in March 2014, providers are not allowed to collect information about the activity of their users unless it is reasonably necessary for business purposes. Consequently, the degree to which individual providers store information is highly variable. The government has identified this variability as a problem which the data retention bill is designed to solve. However, this variability reflects the fact that different businesses have different business requirements. Not all telecommunications providers are alike. Large firms with major infrastructure responsibilities keep larger amounts of data than small firms that resell services. One concern in the debate over data retention is that the government is assuming that the different volumes of data kept by various service providers is a pure function of the preferences of the providers themselves, rather than a reflection of genuine business needs. We shall discuss the political economy consequences of this below.

The upshot of the data retention bill is to try to shoehorn the framework by which law enforcement agencies enjoyed largely unfettered access to billing information onto the internet era. But internet activity and telephone activity are not parallels. They operate under substantially different

[3] Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats,* Government of Australia, Canberra, 2012.

technological paradigms, and they have vastly different social profiles. Where telephone conversations are an adjunct to our lives, internet access is central to it – an enormous amount of interaction with the world is done through the internet. What we do on the internet is part of our private domain to a degree that telephone conversations are not. We live our lives online – to a great degree our work, private lives, our leisure, and our personal and professional relationships are mediated by digital technologies.

The data retention bill requires telecommunications providers to create – not simply store – large and costly databases of customer information related to their activities. The government has released a draft data set which might be retained. The major limitation on this data set is spelled out in the legislation as prohibiting the mandatory retention of website addresses or IP addresses that could amount to web-browsing history. The data set purports to be limited but it does not take much to see that the profile it could create about a person would be incredibly significant. For instance, the IP addresses of mobile phones as they jump from cell tower to cell tower could be used to create a map of everywhere a person has travelled going back two years.

By doing so, the data retention bill drastically and concerningly expands the scope of telecommunications interception, opens up privacy risks, adds a significant regulatory burden onto the telecommunications sector. And yet at the same time, based on international experience, it is unlikely to add substantially to Australia's law enforcement capabilities.

Mandatory data retention is not a targeted national security measure

The government's decision to exclude the vast majority of agencies currently accessing stored communications data without a warrant is a welcome one. The Bill reduces the number of agencies able to access telecommunications data without a warrant to criminal law-enforcement agencies, which include federal and state police, the Australian Crime Commission and state anti-corruption bodies. This is a welcome resolution of the extraordinary breadth of agencies which have had warrantless access to data under the existing Act.

Nevertheless, this is still a broad range of agencies that oversee a large number of law enforcement activities. The Prime Minister Tony Abbott has already suggested that data retention is to be used for "general crime", rather than just national security purposes.[4] The Australian Federal Police Commissioner Andrew Colvin has underlined the wide possible uses for data retention:

> any connection somebody has over the internet, we need to be able to identify the parties to that connection ... So illegal downloads, piracy ... cyber-crimes, cyber-security, all these matters and our ability to investigate them is absolutely pinned to our ability to retrieve and use metadata.[5]

Furthermore, the Bill provides for the Attorney-General to declare any other authority or body to be a criminal law-enforcement agency for the purpose of the Act. These agencies will then enjoy the full access to the new data as other law enforcement agencies. The Australian Securities and Investment Commission has already declared its interest in applying for law enforcement agency status. Much of the political drive for data retention has emanated from regulatory agencies. Both the Australian Taxation Office and the Australian Competition and Consumer Commission have been ferocious advocates of mandatory data retention.[6] There is no reason to believe that this parliament or the next will keep the range of agencies limited under the new legislation.

It is also deeply concerning that mandatory data retention will inevitably be a feature of civil litigation. Any information that is created can be accessed by a subpoena with the permission of a court. While many citizens may believe that democratic governments act in their own best interest most of the time, they might not believe the same about their fellow citizens, who they may have to face in future litigation. This has been the experience of other nations with data retention laws. One investigation of Polish data retention laws found that "more and more often traffic and location data

---

[4] L Bourke & J Massola, 'Data storage could be used to fight 'general crime', Tony Abbott says', *The Sydney Morning Herald,* 6 August 2014. Available at

[5] G Brandis, M Turnbull, D Lewis, & A Colvin, 'Press Conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014', in Editor (ed.)^(eds.), *Book Press Conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, City, 2014.

[6] Australian Taxation Office, *Submission to Joint Parliamentary Committee on Intelligence and Security Inquiry into potential reforms of National Security Legislation*, 2012; Australian Competition & Consumer Commission, *Submission to Joint Parliamentary Committee on Intelligence and Security Inquiry into potential reforms of National Security Legislation*, 2012.

is requested by the parties in civil disputes such as divorce and alimentary disputes."[7] The prospect of a semi-permanent record of travel data being available for personal litigation is unlikely to be welcomed by Australian voters.

Indeed, international experience suggests that mandatory data retention is not used for the most significant crimes. The Austrian government found 56 separate cases between April 2012 and March 2013 where data retained under data retention laws had been useful: "16 thefts, 12 drug cases, 12 cases of stalking, 7 frauds and 9 others" but no cases of terrorism or anything that could constitute a serious national security issue.[8] In Denmark, the Danish Justice Ministry was only able to find two cases were session logging – the full retention of URLs – had been useful in half a decade.[9] Data from the German Federal Crime Agency has shown data retention has no statistically relevant effect on crime or crime clearance rates. Another German study found that blanket data retention "would have made a difference to only 0.002% of criminal investigations".[10] When Germany abandoned its data retention regime in 2010, crime continued a long term decline that had begun before the introduction of data retention.[11]

[7] K Szymielewicz, *Data Retention in Poland: The issue and the Fight,* Panoptykon Foundation, 2012.
[8] M Ermert, 'EU Data retention might not be proportional to risks', 2013, <http://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170>.
[9] T Olander, 'In Denmark, Online Tracking of Citizens is an Unwieldy Failure', *Tech President,* 22 May 2013. Available at http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy.
[10] Cited in European Digital Rights, *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011.
[11] 'German police statistics prove telecommunications data retention superfluous', 2011, <http://www.vorratsdatenspeicherung.de/content/view/455/79/lang,en/>.

Mandatory data retention is a privacy risk

Privacy is a complex and controversial value. There is no philosophical consensus on its definition, nor any consensus on its significance in the pantheon of human rights. Clearly privacy comes up against certain rights – such as freedom of speech – and it is not at all absolute: the right to privacy is not a trump card against security measures, nor does it make any surveillance necessarily illiberal. We cede certain privacy by choice when we participate in society, and we cede it when we form governments in order to protect our other liberties.

Nevertheless, privacy is an absolutely vital liberty which deserves protection and which ought to be prioritised by the government. Privacy is one of the essential liberal virtues. Undermining the private domain – or even inculcating a belief that the private domain might be undermined – threatens the human flourishing which market liberalism seeks to encourage. As I have argued elsewhere,

> [W]e all require privacy to function and thrive. Let's start with the mundane. Obviously we desire to keep personal details safe – credit card details, internet passwords - to protect ourselves against identity theft. On top of this, we seek to protect ourselves against the judgment or observation of others. We close the door to the bathroom. We act differently with intimates than we do with colleagues. We often protect our thoughts, the details of our relationships, our preferences, from prevailing social norms. We compartmentalise. How many people would be uncomfortable with a colleague flipping through their mobile phone – with the window into a life that such access would provide?
>
> Public life is one in which we all play roles, heavily mediated by social norms, assessments or assumptions about the values of our peers. Private life is a respite from that mediated world – a place we can drop our masks, abandon the petty deceptions that are necessary for smooth social interaction.[12]

The value of privacy developed alongside the development of individualism. As human civilisation became wealthier we started to carve out spaces for ourselves, to de-communalise. Private lives and private interests are synonymous. As Wolfgang Sofsky writes, "Privacy is the citadel of personal freedom. It provides defence against expropriation, importunity, and imposition, against power and coercion."[13]

One popular canard about privacy needs to be tackled here. This concerns the claim that privacy is only a concern if individuals have done something wrong: "if you have done nothing wrong you have nothing to hide". Yet this argument assumes that Australian citizens are well-informed about what activity is unlawful, or what activity they might, in the future, become subject to litigation over. Australian society is badly over-criminalised. The Institute of Public Affairs has found more than 100,000 pages of legislation in operation at the Commonwealth level alone. Many of us "do something wrong" without being aware of it. Given the broad proposed and future reach of data retention, this is a serious concern. Furthermore, the argument assumes that laws are always administered fairly and that abuses of power do not occur. None of these assumptions hold up. Certainly they are not strong enough to sustain a substantial violation of all citizens' liberties.

---

[12] C Berg, 'Surveillance and Privacy', *St James Ethics Centre Journal*, no. October, 2014.
[13] W Sofsky, *Privacy : a manifesto*, Princeton University Press, Princeton, 2008.

Data retention is an obvious threat to ideas of a private life. The Bill creates privacy risks from both lawful and unlawful access. Lawful access will grant courts and law enforcement agencies a greater capacity to inquire into the everyday activities of all Australians, with the attendant reduction in the "private-ness" of our lives that this would entail.

However, the mechanism by which mandatory data retention is to be imposed also creates substantial risks of unlawful access. The new vast databases will have to be stored and secured by telecommunications providers themselves. The existence of a database is itself a privacy risk. Unauthorised access is a fact of life; no data is absolutely secure. We have seen many examples of corporate and bureaucratic violations of privacy – either accidental or deliberately caused by malicious staff. For instance, in December 2014 hackers released thousands of credit cards and user accounts of Playstation, Xbox and Amazon.com.[14] Unauthorised access to databases can come from outsiders and insiders. Between 2006 and 2010 more than 1,000 Medicare employees were investigated for spying on personal information.[15] In 2006 Centrelink sacked 100 staff for snooping on private data about Centrelink customers.[16]

These sorts of privacy breaches are incredibly hard to prevent. There are legal consequences for unauthorised access, yet it nevertheless occurs. The only way to truly secure data is to not collect it in the first place. If Parliament goes ahead with the data retention bill, it must be aware that by doing so it opens up new privacy risks to all Australian internet users; privacy risks which they, and their internet service providers, have not consented to.

[14] J Stone, 'Anonymous hackers release 13,000 passwords and credit card details of Amazon, PlayStation and Xbox users', *The Independent,* 27 December 2014. Available at http://www.independent.co.uk/news/world/hackers-release-13000-passwords-and-credit-card-details-of-amazon-playstation-and-xbox-users-9946391.html.

[15] 'Public servants busted for Medicare snooping', *ABC News Online,* 2 March 2010. Available at http://www.abc.net.au/news/2010-03-02/public-servants-busted-for-medicare-snooping/347246.

[16] 'Centrelink staff sacked for spying', *The Sydney Morning Herald,* 23 August 2006. Available at

Mandatory data retention will have a chilling effect on freedom of speech

Privacy and speech are intimately connected. Very little of our speech is intended for public consumption. Ideas about free speech that are based on the rights of small outspoken classes like journalists and public figures are shallow. Most expression in human society is not printed in newspapers or stated in television or Parliament. While protecting that speech is important, it is a narrow sliver of all the speech we ought to protect. And a focus on speech that seeks the widest possible audience – as public speech does – will understate the relationship between privacy and speech.

When we express ourselves we target it at our intended audience. The likelihood of that expression being heard outside that audience will cause us to restrain our speech. We are less likely to speak freely with someone who is known to break secrets than with someone who is known to keep them; we are more open with our loved ones than strangers. The belief that someone else might be listening or might listen in the future effects our expression. One 1975 study found that "the threat or actuality of government surveillance may psychologically inhibit freedom of speech".[17] The legal scholar Louis B Schwartz has emphasised how deeply the sense of privacy and the liberty of speech are intertwined: "Free conversation is often characterized by exaggeration, obscenity, agreeable falsehoods, and the expression of anti-social desires or views not intended to be taken seriously. The unedited quality of conversation is essential if it is to preserve its intimate, personal and informal character."[18]

The potential of surveillance – and there is no doubt that the data retention bill threatens to inculcate a culture of being under surveillance, given its possible breadth and future expansion – to limit freedom of speech is significant. Once the government has introduced this legal regime it is, barring future judicial oversight, unlikely to be repealed, and almost certain to be extended. The so-called "balance between liberty and security" is only ever moved in favour of security.

[17] GL White & PG Zimbardo, *The chilling effects of surveillance: Deindividuation and reactance,* Office of Naval Research, 1975.
[18] LB Schwartz, 'On Current Proposals to Legalize Wire Tapping', *University of Pennsylvania Law Review*, 1954.

Mandatory data retention constitutes a substantial regulatory burden

The cost of mandatory data retention to ISPs is likely to be substantial. The internet service provider iiNet has estimated the cost of implementing data retention to be more than $100 million in new hardware, electricity usage and infrastructure every year. This cost is certain to be borne by consumers, resulting in an "internet tax" of more than $10 extra per customer per month.

This cost will have significant effects on the shape of the telecommunications industry. The cost of regulatory compliance is not evenly distributed among firms of all sizes. It will be relatively more expensive for low-budget telecommunications providers – who do not, and have no business desire to store masses of data currently – to implement the government's full data retention scheme. Regulations favour large incumbent firms over smaller ones. This is why public choice scholars such as George Stigler have pointed out that regulation is not imposed on large firms – it is acquired by them, as a way of raising barriers to entry against smaller competitors.[19] It has been publicly suggested that some large telecommunications firms have informed the government that the cost of implementing data retention will be minimal, or that the data retention is merely a variation of existing practices. Given that this is not true for smaller firms, this seems to be a clear example of the anti-competitive effects of economic regulation.

The goal of Australian telecommunications policy since deregulation has been to encourage competition in both infrastructure and reselling markets. Despite the substantial change to this policy approach brought about by the National Broadband Network, this remains one of the primary goals of telecommunications policy and ought to continue to be so. There is a high degree of likelihood that the large regulatory burden imposed on all telecommunications firms, large and small, will lead to a consolidation within the industry, reducing competition and therefore reducing, in the medium term, the quality of internet access available to Australian consumers.

The Department of Communications has been one of the major contributors to the Abbott government's red-tape agenda. The government's '*Independent cost-benefit analysis of broadband and review of regulation'* outlined the importance of competition in ensuring a dynamic and consumer-focused telecommunications sector, particularly at the infrastructure level.[20] However, that goal is unlikely to be achieved by imposing substantial new regulations with discriminatory costs. As the Harper review into competition policy draft report notes,

> While generally intended to serve other public policy purposes (e.g. health, safety, standards of conduct, consumer protection), regulatory restrictions can nonetheless adversely influence competition — for example, by creating barriers to entry, advantaging some businesses over others, or reducing incentives to compete.[21]

---

[19] GJ Stigler, 'The Theory of Economic Regulation', *Bell Journal of Economics and Management Science*, vol. 2, no. 1, 1971.
[20] M Vertigan, *National Broadband Network Market and Regulation Report* Department of Communications, Canberra, 2014.
[21] I Harper, *Competition Policy Review: Draft Report,* Commonwealth of Australia, Canberra, 2014.

Mandatory data retention is easy to evade

Malcolm Turnbull has correctly identified the ease with which mandatory data retention can be evaded through the use of virtual private networks (VPNs).[22] These services allow users to route all their web traffic through servers in foreign countries. All the information that would be retained under the proposed data retention law would be the volume downloaded and the fact that the internet user had connected to the VPN. *The Australian* reported in August 2014 that the government's announcement of its plans to implement data retention had seen a spike in Australian interest in VPN services.[23]

The law enforcement value of data retention will be seriously eroded by the large scale VPN use. Any mildly sophisticated user is capable of setting up a VPN on their computer or mobile phone. Given that data retention is intended for "serious crime" in the words of the prime minister, it is likely that any serious criminals will deploy VPNs or other data retention countermeasures to prevent law enforcement action. The Institute of Public Affairs has previously identified VPNs as a critical barrier to government internet policy in the domain of copyright infringement.[24] Security and law enforcement agencies – like copyright holders – have to understand how technological adaptation will limit the efficacy of desired new powers.

For instance, one unfortunate consequence of the government's proposed legislation might be the expanded use of VPNs by the general community as they seek to protect their right to privacy. There is some evidence that government regulatory intervention on the internet increases anonymity.[25] This would lower the ability of law enforcement agencies to use the powers they already have, across the board. Larger scale use of VPNs – or other avoidance techniques, like the use of internet cafes or wireless hotspots – might very well compromise existing telecommunications intercept power. This is not something which should be welcome at all, but it is likely to be a major unintended consequence of the data retention proposal.

[22] M Turnbull, 'Keynote address', paper presented to Govhack Red Carpet Awards 2014, 10 August 2014.
[23] C Griffith, 'Australians flock to VPNs to avoid data retention', *The Australian,* 13 August 2014. Available at http://www.theaustralian.com.au/technology/australians-flock-to-vpns-to-avoid-data-retention/story-e6frgakx-1227022957464.
[24] C Berg & S Breheny, *Submission to Australian government Online Copyright Infringement Discussion Paper,* Institute of Public Affairs, 2014.
[25] S Larsson & M Svensson, 'Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorised File-sharing', *Policy & Internet*, vol. 2, no. 4, 2010.

The government already has a new, legislated, yet largely untested alternative to mandatory data retention

The most fundamental objection to the data retention is that it is not a form of targeted surveillance – rather, it treats all Australians as potential suspects of future crimes, and places their privacy at risk as if they were under surveillance.

It is therefore rather remarkable that a targeted measure of surveillance introduced in 2012 remains largely unused. The *Cybercrime Legislation Amendment Bill* (2012), passed in August of that year, introduced a data preservation scheme by which law enforcement agencies can require telecommunications providers to store any existing or new data on specific individuals for up to 90 days. Data preservation notices do not require warrants, however, access to the information stored under a preservation notice may require a warrant. This scheme is proportional and flexible. Most importantly, it does not breach all Australian's privacy indiscriminately. It does not treat all Australians as if they are already suspected of a crime. Yet as the Inspector-General of Intelligence and Security has determined, in 2013-14 there were "a very small number of such notices raised by ASIO."[26]

If the data preservation scheme under the Bill is inadequate, the government needs to explain why it is so. Given the newness of the scheme, its inadequacy is not clear. Furthermore, if the data preservation scheme is inadequate to face the challenge at hand, can it be adjusted or reformed in order to resolve the challenges of online crime? For instance, is the retention timeframe too short, or too unwieldy for law enforcement agencies? The urgency with which the data retention bill is being pushed through the Parliament should not mean that existing measures in telecommunications intercept law be critically assessed. If the targeted data preservation scheme requires reform, that would be a more privacy-protecting approach than the indiscriminate mass data retention proposal on the table.

[26] Inspector-General of Intelligence and Security, *Annual Report 2013-2014,* Commonwealth of Australia, 2014.

Conclusion

The data retention bill represents dangerous overreach. By threatening all Australians' privacy, it is disproportionate. It is more than just a national security measure, and data retained under the scheme will almost certainly become a feature of civil litigation. It will reshape the competitive structure of the Australian telecommunications sector. As it will spark technological adaptation, it is unlikely to be effective, and also likely to have a counterproductive effect on trying to catch those who would try to hide from law enforcement.

Bibliography

Attorney-General's Department, *Equipping Australia Against Emerging and Evolving Threats,* Government of Australia, Canberra, 2012.

Australian Competition & Consumer Commission, *Submission to Joint Parliamentary Committee on Intelligence and Security Inquiry into potential reforms of National Security Legislation*, 2012.

Australian Taxation Office, *Submission to Joint Parliamentary Committee on Intelligence and Security Inquiry into potential reforms of National Security Legislation*, 2012.

Berg, C, 'Anti-Terrorism Law Reform Follows Legislate In Haste, Repeal At Leisure Approach', *The Sunday Age,* 7 December 2014. Available at http://www.theage.com.au/comment/antiterrorism-law-reform-follows-legislate-in-haste-repeal-at-leisure-approach-20141206-11zz4h.html.

———, 'Surveillance and Privacy', *St James Ethics Centre Journal*, no. October, 2014.

Berg, C & S Breheny, *Submission to Australian government Online Copyright Infringement Discussion Paper,* Institute of Public Affairs, 2014.

Bourke, L & J Massola, 'Data storage could be used to fight 'general crime', Tony Abbott says', *The Sydney Morning Herald,* 6 August 2014. Available at

Brandis, G, M Turnbull, D Lewis, & A Colvin, 'Press Conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014', in Editor (ed.)^(eds.), *Book Press Conference announcing the introduction of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, City, 2014.

'Centrelink staff sacked for spying', *The Sydney Morning Herald,* 23 August 2006. Available at

Ermert, M, 'EU Data retention might not be proportional to risks', 2013, <http://policyreview.info/articles/news/eu-data-retention-might-not-be-proportional-risks/170>.

European Digital Rights, *Shadow evaluation report on the Data Retention Directive (2006/24/EC)*, 2011.

'German police statistics prove telecommunications data retention superfluous', 2011, <http://www.vorratsdatenspeicherung.de/content/view/455/79/lang,en/>.

Griffith, C, 'Australians flock to VPNs to avoid data retention', *The Australian,* 13 August 2014. Available at http://www.theaustralian.com.au/technology/australians-flock-to-vpns-to-avoid-data-retention/story-e6frgakx-1227022957464.

Harper, I, *Competition Policy Review: Draft Report,* Commonwealth of Australia, Canberra, 2014.

Inspector-General of Intelligence and Security, *Annual Report 2013-2014,* Commonwealth of Australia, 2014.

Larsson, S & M Svensson, 'Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorised File-sharing', *Policy & Internet*, vol. 2, no. 4, 2010, 77-105.

Olander, T, 'In Denmark, Online Tracking of Citizens is an Unwieldy Failure', *Tech President,* 22 May 2013. Available at http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy.

'Public servants busted for Medicare snooping', *ABC News Online,* 2 March 2010. Available at http://www.abc.net.au/news/2010-03-02/public-servants-busted-for-medicare-snooping/347246.

Rodrick, S, 'Accessing Telecommunications Data for National Security and Law Enforcement Purposes', *Federal Law Review*, vol. 37, no. 3, 2009, 375.

Schwartz, LB, 'On Current Proposals to Legalize Wire Tapping', *University of Pennsylvania Law Review*, 1954, 157-67.

Sofsky, W, *Privacy : a manifesto*, Princeton University Press, Princeton, 2008.

Stigler, GJ, 'The Theory of Economic Regulation', *Bell Journal of Economics and Management Science*, vol. 2, no. 1, 1971, 3-21.

Stone, J, 'Anonymous hackers release 13,000 passwords and credit card details of Amazon, PlayStation and Xbox users', *The Independent,* 27 December 2014. Available at http://www.independent.co.uk/news/world/hackers-release-13000-passwords-and-credit-card-details-of-amazon-playstation-and-xbox-users-9946391.html.

Szymielewicz, K, *Data Retention in Poland: The issue and the Fight,* Panoptykon Foundation, 2012.

Turnbull, M, 'Keynote address', paper presented to Govhack Red Carpet Awards 2014, 10 August 2014.

Vertigan, M, *National Broadband Network Market and Regulation Report* Department of Communications, Canberra, 2014.

White, GL & PG Zimbardo, *The chilling effects of surveillance: Deindividuation and reactance,* Office of Naval Research, 1975.