MACQUARIE University

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

Prepared by:

Dr John Selby
Prof. Vijay Varadharajan
Dr Yvette Blount

Summary

We agree with and support the civil liberties and technical concerns raised in other submissions to this Joint Committee. In addition, this Bill poses significant risks for Australian businesses and the integrity of its financial markets. Those risks should be fully explored with relevant stakeholders prior to the consideration of this Bill by the Parliament. Our recommendations are:

Recommendation [1]: Division 2 of Part 5-1A of the Bill or any proposed Regulations be amended to include requirements that:

1) Each Service Provider is required to create an aggregated risk profile of its business customers;
2) Service Providers must implement a level of security sufficient to protect the metadata sensitive to their most-at-risk business customers; and
3) the decision to approve a data retention plan should include analysis of whether a service provider has implemented a level of security sufficient to protect metadata sensitive to their most-at-risk business customers (rather than the precautions necessary to protect the average risk exposure of their business customers)

Recommendation [2]: Prior to this Bill being voted upon by the Parliament, broad consultation with business, industry and other stakeholders should occur to determine which business stakeholders are at risk and could suffer damage when retained business metadata is unlawfully accessed by third parties.

Recommendation [3]: the Bill should include a requirement that Service Providers must promptly notify relevant regulators (such as ASIC) and all customers of any detected unauthorised access to their retained metadata pools and of what steps have been taken to fix any security flaws that have been detected.

Recommendation [4]: Row 5(a) of the Proposed Data Set be amended to state “non web-based (i.e. not http:// or https://) chat, forum, social media”

Recommendation [5]: Row 5 (b) of the Proposed Data Set should be re-examined to state explicitly which Wi-Fi services will be subject to the Bill; who is classified as a Service Provider of Wi-Fi and to clearly state how such Service Providers will be identified.

Recommendation [6]: Schedule 3 of the Bill be amended to include specific funding for the Commonwealth Ombudsman to be able to properly deliver on its supervisory role. The Inspector-General of Intelligence and Security should also receive specific funding so as to be able to properly deliver on its supervisory role.

Recommendation [7]: Sub-sections 110A(1)(m) and 110A(3)-(9) of the Bill should be deleted.

Recommendation [8]: The Proposed Data Set for the Data Retention Bill should not form part of the Regulations of the Bill, instead the Proposed Data Set should be included as a section within the Bill itself.

16 January 2015

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
Parliament House
CANBERRA ACT 2600

Dear Secretary,

Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

Thank you for the opportunity to make a submission to this inquiry. We do so in our capacity as academics at Macquarie University. We are solely responsible for the views and content in this submission.

This Bill raises significant issues affecting both national security and civil liberties, such as privacy, topics which have been extensively covered in the various other submissions made to this Inquiry, including those by the Gilbert + Tobin Centre of Public Law at the University of New South Wales and the Communications Alliance/AMTA. On those topics, we generally agree with and support the positions expressed within those submissions. Rather than simply re-stating that agreement, we have chosen to focus our attention on several additional matters not contained within those submissions.

1) Risks to Australian Business from Metadata Retention should be explicitly included within the Cost-Benefit Analysis for this Bill

This issue is related to Recommendations 2 and 6 of Chapter 2 of the 2013 Report of the Inquiry into Potential Reforms of Australia's National Security Legislation.

Whilst most of the public debate over this Bill has focused upon the need to balance the need to protect civil liberties in a modern, Western liberal democracy (such as privacy and the general presumption of innocence) against national security risks, the metadata which would be retained under this Bill includes communications not only by individuals (which in itself raises many significant issues addressed in other submissions), but also communications by Australian businesses. Whilst the importance of protecting the confidentiality of the contents of those business communications is relatively obvious, the importance of protecting the confidentiality of metadata about who in a business is talking to which advisors, when, and how often has not yet formed a significant part of the public debate about this Bill.

Listed companies and their business advisors already face direct attacks by unauthorised third parties seeking to gain access to their communications for

illegal purposes (such as insider trading).[1] As currently drafted, this Bill risks creating an *indirect* vector for attacks against Australian listed companies and their business advisors capable of causing significant harm to the integrity of Australia's financial markets due to a reduced opportunity to detect insider trading.[2]

s187A of the current Bill requires Service Providers to collect and store the metadata of their customers (who consist of both individuals and businesses).[3] Consequently, metadata about business communications would be retained outside of the existing internal data protection systems put in place by those Australian businesses to protect their own data. These Service Providers may simultaneously retain the business communications metadata of hundreds, even thousands, of different businesses and thus will be unlikely to be able to accurately determine the appropriate level of data security needed for the metadata for each of those businesses.

As the cost of adequately securing data rises exponentially as the value of that data increases and it is widely recognised that "information systems are prone to fail when the person responsible for protecting a system is not the one who suffers when it fails"[4], it is unlikely that Service Providers will, on their own, invest sufficient funds to adequately protect the most sensitive metadata of their business customers (it being impractically expensive for a telecommunications service provider to determine the relative risk faced by each of their customers).[5]

[1] For example, American listed companies, Wall Street law firms and investment banks have been under direct attack since 2013 by the Fin4 Group which has exploited illegally-accessed business communications so as to engage in insider trading of pharmaceutical stocks: FireEye, 'Hacking the Street: Fin4 Likely Playing the Market' <http://www2 fireeye.com/fin4 html>

[2] Investing resources to detect the direct vectors by which a person is able to gain the information used to engage in insider trading is the typical way to increase the probability of catching such criminals. See, for example, the 2014 prosecutions of Lukas Kamay and Christopher Hill for insider trading based upon access to undisclosed Australian Bureau of Statistics data. The direct connection between Kamay and Hill was first identified through their connected LinkedIn profiles.

[3] We recognise that the metadata retained about the communications of most business customers of Service Providers is not going to be suitable for such criminal exploitation – the metadata for business communications from a local pie shop are going to be far less sensitive in nature than the metadata for business communications between an ASX-listed company and its advisors, such as the mergers and acquisitions / bankruptcy teams within its law firms / accountants / investment banks. Whilst the pie shop owner, the ASX-listed company, the law firms, accountants and investment banks could all potentially have the same telecommunications service provider, the economic value of the risk of unauthorised third-party access to their metadata varies from insignificant to potentially hundreds of millions of dollars.

[4] Tyler Moore and Ross Anderson, 'Economics and Internet Security: A Survey of Recent Analytical, Empirical and Behavioral Research' *Harvard University Computer Science Group Research Paper TR-03-11* <ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf>

[5] s187D of the Bill sets out the requirement for Service Providers to prepare and have approved a "data retention plan".

Recommendation [1]: Division 2 of Part 5-1A of the Bill or any proposed Regulations be amended to include requirements that:
1) Each Service Provider is required to create an aggregated risk profile of its business customers;
2) Service Providers must implement a level of security sufficient to protect the metadata sensitive to their most-at-risk business customers; and
3) the decision to approve a data retention plan should include analysis of whether a service provider has implemented a level of security sufficient to protect metadata sensitive to their most-at-risk business customers (rather than the precautions necessary to protect the average risk exposure of their business customers)

Another factor that would influence the level of security provided by Service Providers is the risk of being sued (tort liability) for negligence if the retained metadata of one (or more) of their customers is accessed by unauthorised third parties. For example, in New South Wales, under s5B of the Civil Liability Act a telecommunications service provider is only liable if they failed to take precautions against a risk of harm that was "foreseeable, not insignificant and a reasonable person in their position would have taken those precautions".

The economics of security are, unfortunately, unfavourable to Service Providers in this context.[6] The cost of taking sufficient precautions to defend against attackers seeking to gain access to the most valuable stored business metadata is much higher than the cost of launching such attacks and such precautions may be inherently inadequate.

For example, an unauthorised third party who sought to gain access to a telecommunications service provider's pool of retained metadata might take advantage of the rise of "zero-day markets".[7] These markets are online venues through which previously un-identified flaws and exploits in computer hardware, operating systems and software are traded. The price for such flaws and exploits varies depending upon the extent to which access is gained, but commonly ranges from $USD50 000 to $USD250 000.[8] As these flaws and exploits are not yet known by the manufacturers of the hardware, operating systems and software (hence the term zero-day) used by Service Providers to protect the retained metadata of their customers, they are unlikely to be detected by the typical computer security counter-measures, such as firewalls, intrusion detection systems and anti-virus detection software. In short, these zero-day exploits are a readily available and relatively cheap tool which could be used by a cyber-criminal to

[6] See, for example, Huw Fraser, Roskana Moore and Tim Chown, 'On the Viability of Using Liability to Incentivise Internet Security' *Paper Presented to the Twelfth Workshop on the Economics of Information Security (WEIS 2013 Conference, Georgetown University, Washington D.C. 11-12 June 2013)* <http://weis2013.econinfosec.org/papers/FryerMooreChownWEIS2013.pdf>.
[7] Serge Egelman, Cormac Herley and Paul van Oorshot, 'Markets for Zero-Day Exploits: Ethics and Implications' *NSPW '13 Proceedings of the 2013 Workshop on New Security Paradigms* pp41-46, <http://people.scs.carleton.ca/~paulv/papers/NSPW-2013-author-version.pdf>
[8] Andy Greenberg, 'Shopping for Zero-Days: A Price List for Hackers' Secret Software Exploits' Forbes Magazine 23 March 2012 <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>

tunnel directly into a telecommunications service provider's pool of retained business metadata.

As a zero-day exploit is, by definition, not something against which precautions could reasonably be taken, an Australian business (or its shareholders) who have suffered losses due to insider trading by unknown third parties on the basis of unlawfully accessed business metadata would be unlikely to satisfy the legal requirements necessary to recover such losses from the telecommunications service provider by suing them on the basis of a statutory tort of negligence.

Recommendation [2]: Prior to this Bill being voted upon by the Parliament, broad consultation with business, industry and other stakeholders should occur to determine which business stakeholders are at risk and could suffer damage when retained business metadata is unlawfully accessed by third parties.

If the expected value of such an attack (the probability of being caught multiplied by the value of insider-trading on the information which can be extracted from that business metadata) exceeds the cost of gaining access to such business metadata (i.e. buying and deploying a suitable zero-day exploit against a telecommunications service provider), then unauthorised third parties are likely to launch such attacks.

One consequence of such indirect attacks is that it reduces the ability to detect crimes such as insider trading. Two factors lower the probability of being caught for insider trading on information gained from unauthorised access to retained business metadata when compared to a direct attack against a listed company or business advisory firm. First, Service Providers are likely to aggregate their customers' retained metadata, making it much harder to determine which of the thousands of those business customers' metadata was of interest to the attackers. Second, as discussed above, the use of zero-day exploits may permit the attackers to access the retained business metadata without being detected. Thus, there may be no direct connection between a criminal engaging in such insider trader, the listed company or its advisors.

Another consequence of the indirect nature of the attack on retained business metadata is the potential for it to undermine trust between Australian listed companies and their business advisors. In a similar situation, the Leveson Inquiry into press ethics in the UK heard evidence of how such trust was undermined when UK journalists surreptitiously intercepted voicemails left by celebrities (such as Elle McPherson) and their advisors.[9] If, for example, a listed company were to only reveal their intention to undertake a takeover of another listed company to one advisory firm, but shortly thereafter an unauthorised third party engaged in insider trading on the basis of detecting that flurry of communication within a pool of retained metadata, the listed company might inaccurately suspect its advisory firm of being the source of a leak that moved the target's share price before any public announcement had been released. Whilst the advisory firm may

[9] Lord Justice Leveson, 'An Inquiry into the Culture, Practices and Ethics of the Press' Vol. 1, p306; Stuart Jeffries, 'The Truth About Elle and Me' *The Guardian Newspaper* 26 November 2011, <http://www.theguardian.com/theguardian/2011/nov/26/mary-ellen-field-macpherson-leveson>

protest its innocence and neither business could detect any direct attacks against their internal IT systems, the insider trading may still occur.

Therefore, we believe that it is important for the Committee to investigate thoroughly the potential risks and their consequences for Australian businesses from the creation of pools of business metadata by Service Providers.

Recommendation [3]: the Bill should include a requirement that Service Providers must promptly notify relevant regulators (such as ASIC) and all customers and end users of any detected unauthorised access to their retained metadata pools and of what steps have been taken to fix any security flaws that have been detected.

We are currently negotiating with industry partners to conduct a pilot study to quantify these risks and can share the findings of that research with the Committee when it is completed. An example may help illustrate these risks:

We conjecture that an ill-intentioned third party could exploit an insufficiently-secured metadata retention scheme in the following manner:

1) Identify Internet Service Providers (ISPs) that are storing the email metadata of listed companies / investment banks;
2) Identify the network devices / hardware /operating systems and software used by the target ISP that insufficiently protect retained email metadata;
3) Purchase from a zero-day exploit market website a zero-day exploit targeted at the relevant network devices / hardware / operating system and/or software identified in Step 2) (estimated cost $50 000 - $250 000);
4) Either launch the attack themselves or obfuscate their identity by hiring a third party to launch the zero-day attack on the target ISP;
5) Gain unauthorised access to the target ISPs' retained email metadata pool (including up to two years of the listed company's/advisory firms' correspondence);
6) Download a copy of that metadata pool so as to undertake remote analysis / undertake searches using the ISP's own search tools used to provide reports to law enforcement agencies;
7) Identify relevant Mergers & Acquisitions/bankruptcy advisors from LinkedIn profiles / advisory firm websites;
8) Undertake a traffic analysis of the email metadata pool to identify increases in volumes of correspondence between those M&A/bankruptcy teams in advisory firms and executives in listed companies;
9) Identify potential ASX-listed insider-trading targets;
10) Back-test financial market trading strategies based upon historical data within the metadata pool to optimise potential returns;
11) Apply those trading strategies to the most recent events identified by the metadata traffic analysis (i.e. those M&A/Bankruptcy deals which have not yet been made known to market participants);
12) Reap out-sized profits at reduced risk of being caught for insider trading.

2) Other issues:

a. Under Row 5(a) (the type of communication or relevant service used in connection with a communication) of the Proposed Data Set for the Data Retention Bill released by the Department includes examples such as "chat, forum and social media". With such services, the notion of what metadata constitutes is much more than just source and destination, etc. The metadata incudes a variety of contextual information which help to identify the various attributes involved in transactions and scenarios. This can potentially lead to several privacy as well as security issues. Many chat services, forums and social media sites are accessed over the World Wide Web (WWW) through the hypertext transfer protocol (HTTP), i.e. are accessed whilst a person is "web-browsing". The retention of metadata about the usage of internet-based chat services, forums and social media would require the monitoring of all web-browsing by customers so as to separate out and retain metadata relating to web-based chat services, forums and social media. This appears to contradict s187B(4) of the Bill as that section prohibits Service Providers from retaining subscribers "web browsing history".

Recommendation [4]: Row 5(a) of the Proposed Data Set be amended to state "non web-based (i.e. not http:// or https://) chat, forum, social media".

b. Under Row 5(b) of the Proposed Data Set, Wi-Fi is listed as a relevant service. The vast majority of Wi-Fi services in Australia are privately operated by families in their homes or businesses in their workplaces. Those Wi-Fi services are not provided by Service Providers and details about the private Wi-Fi access points operated by families in their homes and businesses in their workplaces should not be retained by Service Providers. At a maximum, only metadata about public Wi-Fi services operated and controlled by the Service Providers themselves should be retained.

Recommendation [5]: Row 5 (b) of the Proposed Data Set should be re-examined to state explicitly which Wi-Fi services will be subject to the Bill; who is classified as a Service Provider of Wi-Fi and to clearly state how such Service Providers will be identified.

c. Whilst Schedule 3 of the Bill grants oversight powers to the Commonwealth Ombudsman, the Bill does not include specific provisions for additional funding for the Commonwealth Ombudsman so as to be able to adequately resource its new oversight task. Oversight without sufficient resources provides only the illusion of scrutiny, rather than the actual scrutiny necessary to determine whether the intrusive powers being granted to government agencies by this legislation are being used in a limited, proper manner, and not being abused.

Recommendation [6]: Schedule 3 of the Bill be amended to include specific funding for the Commonwealth Ombudsman to be able to properly deliver on its supervisory role. The Inspector-General of Intelligence and Security should also receive specific funding so as to be able to properly deliver on its supervisory role.

d. Over time, there is significant risk of scope-creep within this legislation. Consequently, we believe that is not advisable to grant significant discretions within the Bill. We are particularly concerned about the discretions available to the Attorney-General (particularly some unknown future A-G) to 1) grant access to metadata to additional government agencies; and 2) to expand the types of communications about which metadata that will be retained.

   Whilst Regulations are disallowable instruments, by default they are accepted-until-rejected. This is the opposite of the position regarding sections within legislation, wherein proposed amendments are rejected-until-accepted. Therefore, given the intrusive nature of this legislation and its potential for abuse by future governments, we believe that the precautionary principle should apply and discretions should be minimised within the Bill.

Recommendation [7]: Sub-sections 110A(1)(m) and 110A(3)-(9) of the Bill should be deleted.

Recommendation [8]: The Proposed Data Set for the Data Retention Bill should not form part of the Regulations of the Bill, instead the Proposed Data Set should be included as a section within the Bill itself.

***

Improvements to the Bill in these areas would significantly reduce the negative un-intended consequences of this proposed legislation.

Yours sincerely,

Dr John Selby
Prof. Vijay Varadharajan
Dr Yvette Blount