Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600

Dear Secretary

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

Please find enclosed a submission to the Committee's inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.

I make this submission in a private capacity and in no way intend to reflect the views of my employers, Private Media.

Yours sincerely

Bernard Keane

Canberra

14 January 2015

Introduction

The referral of the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (the Bill) to the Committee by the Attorney-General follows inquiries by the Committee into other bills expanding the powers of the government and its agencies in relation to counter-terrorism in 2014. The Attorney-General is to be commended for continuing the practice established under the previous government of seeking the Committee's assessment of proposed changes to national security laws prior to passage through Parliament.

This is the second time in just over two years that the Committee has considered the issue of data retention. The previous inquiry, into Potential Reforms of National Security Legislation, the report of which was tabled in the previous Parliament, addressed several of the key issues arising from a proposed data retention régime and received a large volume of submissions from stakeholders and ordinary voters concerned about such a régime.

In the period since the previous inquiry, it has become still more clear that data retention is a profoundly flawed approach to law enforcement and intelligence-gathering. In the European Union, previously held by advocates of mass surveillance as an example of the successful implementation of data retention, data retention has been found to be illegal and abandoned. Further evidence has emerged of its ineffectiveness and of the threat it poses to core democratic practices and free speech. And in the Australian context, the lack of oversight and accountability for intelligence and law enforcement agencies has emerged as a significant issue.

This submission outlines the key flaws of the government's proposed data retention scheme.

1. It remains unclear what data is supposed to be retained

In its June 2013 report on its Inquiry into Potential Reforms of National Security Legislation, the Committee specifically criticised the Attorney-General's Department (AGD) for its unwillingness to provide a definition of what data was to be retained under a data retention regime, and the fact that an extensive discussion paper on national security reforms had devoted barely a sentence to the data retention proposal.

> *This lack of information from the Attorney-General and her Department had two major consequences. First, it meant that submitters to the Inquiry could not be sure as to what they were being asked to comment on. Second, as the Committee was not sure of the exact nature of what the Attorney-General and her Department was proposing it was seriously hampered in the conduct of the inquiry and the process of obtaining evidence from witnesses.*
>
> *Importantly the Committee was very disconcerted to find, once it commenced its Inquiry, that the Attorney-General's Department (AGD) had much more detailed information on the topic of data retention. Departmental work, including discussions with stakeholders, had been undertaken previously. Details of this work had to be drawn from witnesses representing the AGD.*
>
> *In fact, it took until the 7th November 2012 for the Committee to be provided with a formal complete definition of which data was to be retained under the data*

retention regime proposed by the AGD.

What the Committee report did not note, possibly out of politeness, was that AGD had not even provided its definition (essentially the EU data retention directive definition) to the Committee first, but instead had produced it at Estimates hearings to a non-Committee member, Senator Ludlam.

According to documents obtained under Freedom of Information laws, AGD has been working on data retention since at least 2008. There is no clear reason why it should not have been able to produce a detailed definition prior to the 2012-13 inquiry, especially given that as part of its work on the issue, it had conducted an extensive round of industry consultation, taken the matter to Cabinet and prepared draft legislation and a draft Regulatory Impact Statement. Nonetheless, given the Committee's criticism of AGD in the previous inquiry, it would be reasonable to expect that AGD would *this time* have a formal and finalised definition for the Committee's consideration.

This has, regrettably, not been the case. Despite further rounds of consultation with industry and the involvement of consultant PWC, AGD has *still* been unable to determine what internet metadata it wants to compel communications companies to retain in addition to telephone data. There is no definition in the Bill; the definition has been left to be finalised via regulation, with a technical working group, headed by the Secretary of AGD, tasked to finalise what, apparently, AGD has been unable to finalise for almost seven years.

That working group provided the Committee with a *draft* definition in mid-December, but it remains unfinalised and in its first hearing, the Committee was unable to extract a commitment from AGD that it would even be finalised before the current inquiry reporting data in February.

AGD's refusal to provide a definition to the Committee after seven years of work, and its refusal to provide a definition before this inquiry is scheduled to be completed, is disrespectful, if not openly contemptuous, of the Committee, the Parliament and stakeholders. The Committee simply cannot undertake an effective inquiry into data retention, nor can stakeholders make appropriate submissions to such an inquiry, if *the* key question cannot be addressed.

As a consequence of the lack of a definition of what data will need to be retained, at the inquiry's first hearing in December, AGD officials were also unable to advise the Committee of what the data retention scheme would cost, a remarkable admission given the bill is currently before Parliament and long-standing legislative processes under governments of both sides have required Regulatory Impact Statements to identify impacts on business. As with the definition of retained data, it appears costings may not be finalised until the Committee has reported. Again, this significantly impairs the capacity of stakeholders, and in particular the targets of the proposed régime, communications companies, to comment meaningfully on a key question before the Committee.

It is also unclear how the costs will be allocated between business and government, with only an assertion from the government that it may bear some of the costs – at the minimum, likely to be tens of millions of dollars. However, unless the government bears the *full cost* of data retention, the cost burden placed on communications companies and therefore, inevitably, on

consumers, will in effect be a surveillance tax in which consumers will be forced to pay for their own government to place them under surveillance.

What has emerged about the data definition, however, is that government ministers have misled the public about what it will entail. The Minister for Communications has repeatedly claimed that the régime proposed under the Bill will not require communications companies to retain any data beyond that which they currently retain. On 30 October, that Minister stated at a media conference "the important thing to understand about this metadata bill, these amendments, is that it is not creating new classes of data to be retained… it's about preserving the status quo."

This claim was easily debunked by the company iiNet in its response to the government's own industry consultation paper. As iiNet noted,

> *"The Consultation Paper expressly states that data which falls within the defined data set will be required to be retained 'even if this exceeds business needs' and that 'the policy recognises that providers may need to modify some systems to ensure they meet the minimum standard'."*

Further, in October, Telstra stated in its response to the bill that "complying with the legislation will go beyond Telstra's current business practices".

The responses of iiNet and Telstra were confirmed by officials in their appearance before the Committee in December, when they noted that some ISPs would have to create data, rather than merely, as the government has insisted, store existing data. Industry representatives subsequently confirmed this at the same hearing.

2. By any definition data retention doesn't work

The justification for mass surveillance régimes of any kind, including data retention, is that they enhance the ability of law enforcement and intelligence agencies to detect, prevent and investigate terrorism and crime, and ward off the threat of "going dark" (that is, losing the capacity to obtain data on communications use as communications companies alter business practices to take advantage of digital technologies to reduce costs). Government ministers have made much of this justification, emphasising that data retention is only aimed at serious crimes, although there are no such restrictions giving effect to this in the bill, and indeed the Commissioner of the Australian Federal Police has stated that the AFP will use data retention to pursue filesharing, which is currently dealt with under civil law.

However, advocates of data retention are unable to point to *any* evidence that it provides any benefits in relation to crime or terrorism, no matter how broadly defined. A German parliamentary study concluded data retention in Germany (before it was ruled illegal) had led to an increase in the crime clearance rate of 0.006% (sic).[1]

[1] http://www.vorratsdatenspeicherung.de/content/view/446/79/lang,en/, accessed 5 Jan 2015

Danish police have said data retention – which in that country involves the retention of internet browsing histories – has not had any benefit in solving crimes – the information proved too unwieldy to use.[2]

Most significantly, the review panel established by President Barack Obama into the revelations of whistleblower Edward Snowden about the mass surveillance activities of the National Security Agency in the United States – programs that went well beyond data retention to a comprehensive system of collection of content and metadata from internet and phone use – similarly show no benefit. The panel reported that it couldn't find *any* evidence that the results of the NSA's mass surveillance had been necessary to stopping any terrorist attacks. The panel had looked for evidence the NSA's data had stopped any attacks "that might have been really big. We found none," said one panel member.[3]

Indeed, the recent history of terrorism in Western countries, from the United States, to Australia, to France, has been that perpetrators have been well-known to authorities prior to attacks, or authorities have been warned about them, but failed to take action to prevent attacks. The problem has not been a lack of intelligence, but instead a lack of effective preventive action by agencies.

3. Data retention creates the very problem it is intended to fix

The demonstrated failure of data retention to achieve any improvements in counter-terrorism or crime-fighting capability makes intuitive sense: there are ample encryption and anonymisation tools that ordinary consumers, let alone serious criminals and terrorist networks, use to ensure their internet usage and online identities cannot be tracked by ISPs or government bodies, which is the entire point of data retention. Such tools are also critical to activists living in countries with repressive regimes, and the US government has specifically encouraged and funded internet anonymity as a key tool for democracy activists, despite understanding that such tools could also be used for malign purposes. As then-Secretary of State Hillary Clinton said in 2010,

> *Those who use the internet to recruit terrorists or distribute stolen intellectual property cannot divorce their online actions from their real world identities. But these challenges must not become an excuse for governments to systematically violate the rights and privacy of those who use the internet for peaceful political purposes… We are also supporting the development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship. We are providing funds to groups around the world to make sure that those tools get to the people who need them in local languages, and with the training they need to access the internet safely.*[4]

Defeating data retention online via use of, for example, VPNs or the Tor network, is relatively straightforward and increasingly common. Indeed, data retention is likely to prove

---

[2] http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy, accessed 5 Jan 2015

[3] http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588, accessed 5 Jan 2015

[4] http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm, accessed 13 Jan 2015

a spur to ordinary internet users to use VPNs or other online anonymisation and encryption tools to protect themselves from government and corporate surveillance. This has already proven to be the case following the Snowden revelations about the NSA. In the last 18 months, the United States' biggest IT and internet companies have moved to offer greater privacy protections. In November 2014, WhatsApp announced it was embedding end-to-end encryption in its messaging service, making messages unreadable even by the company itself, and Facebook pledged support for Tor. In September, Apple revealed encryption on iPhone 6s and new iPads would be in place by default and the company would not hold the encryption keys, so it would be unable to provide them to security agencies. Google followed Apple with a similar announcement about the next version of Android. In August, Yahoo announced it was working on end-to-end encryption, using the OpenPGP standard, for its webmail service with Google, so that Yahoo and Gmail users will be able to email one another securely. In July, Microsoft announced it would improve encryption in Outlook and that it would make its code available so that users could inspect it to check there were no government backdoors in it .

Since the Snowden revelations, there has been a growing appetite for encryption and anonymisation products. Usage of Tor spiked in 2013[5] in the wake of the Snowden revelations, and since then has plateaued at a level twice that of pre-2013, despite constant claims Tor has been successfully tapped by security agencies. In Australia, around 30,000 users are currently connecting to Tor, three times the 2013 level, and the number is rising; US numbers show the same pattern, but at level tenfold that of Australia.[6] In May 2014, Essential Research found at least 30% of Australians were taking some measures to stay anonymous online.[7]

The current push for data retention in Australia will merely repeat the surge of interest in encryption and anonymisation caused by the revelations of NSA mass surveillance around the world. In pushing for data retention, AGD, law enforcement and intelligence agencies will merely have created a real version of "going dark".

4. The "going dark" argument is misleading

It is also important to note that the "going dark" argument put forward by law enforcement and intelligence agencies (which in any event is undermined by AGD's admission that data retention will impose *new* data requirements on communications companies) is misleading. The comparison between traditional telephony data and the data to be retained under any but the most minimalist data retention definitions illustrates this, especially in relation to mobile phone data.

Mobile phone data includes location as a phone interacts with nearby phone towers, so in effect phone data can be used to track an individual's movements. However, in spite of the bizarre and patently misleading use of an "envelope" metaphor by government ministers in relation to metadata, it is the compilation of such data that enables agencies to access far more information about an individual than could ever have been provided even under traditional wiretapping of an individual's phone calls.

---

[5] https://nakedsecurity.sophos.com/2013/08/29/tor-usage-doubles-in-august-new-privacy-seeking-users-or-botnet/, accessed 13 Jan 2015
[6] https://metrics.torproject.org/userstats-relay-country.html, accessed 13 Jan 2015
[7] http://essentialvision.com.au/actions-taken-to-protect-privacy, accessed 13 Jan 2015

With sufficient metadata, agencies can accumulate a record of everyone an individual has called, everyone those people have in turn called, how long they spoke for, the order of the calls, and where an individual was when they made the call, to build a profile that says far more about that person than overheard phone calls or copies of emails. It can reveal not just straightforward details such as friends and acquaintances, but also if an individual has medical issues, their financial interests, what they are buying and their personal relationships. Combined with other publicly available information, having a full set of metadata on an individual will tell agencies far more than much of their content data ever will.

This is openly acknowledged by a disparate group of intelligence figures. The General Counsel for the NSA has publicly stated, "metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content." According to the former head of the NSA, Michael Hayden, the US government kills people based on metadata it has accumulated on them.[8] And as Edward Snowden has said: "you can't trust what you're hearing, but you can trust the metadata."[9]

5. Despite the "going dark" argument, existing tools to address it aren't used

The "going dark" argument is further undermined by the fact that ASIO simply doesn't use existing tools designed explicitly to enable data retention.

For two years, ASIO, the AFP and state police forces have had the power, under the *Cybercrime Legislation Amendment Act 2012*, to require communications companies to store information that may help in the investigation of a "serious contravention" — an offence punishable by three years or more in jail — for up to 90 days before getting a warrant to access the data. The only limitation on the requests apart from the seriousness of the offence is that it must be targeted at one person, but an agency can issue as many preservation notices as necessary.

According to the Inspector-General of Intelligence and Security's 2013-14 annual report, however, during that year, "there was a very small number of such notices raised by ASIO." Prominent internet service provider iiNet has repeatedly argued that there has been no explanation from the government or agencies for why an additional data retention regime over and above the preservation notice regime is needed, or what flaws exist in the preservation notice system, which is barely two years old, that render it problematic for agencies.

6. The proposed two year retention period is unsupported by evidence

To this point, neither the government nor AGD and its agencies have provided any evidence justifying the two year retention period proposed in the Bill. The EU data retention directive, on which the government has relied so heavily in other areas, specified a minimum retention period of just six months, and a *maximum* period of two years. Six months is more than

---

[8] https://www.techdirt.com/articles/20140511/06390427191/michael-hayden-gleefully-admits-we-kill-people-based-metadata.shtml, accessed 13 Jan 2015

[9] http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript, accessed 13 Jan 2015

ample for law enforcement purposes: data from the United Kingdom shows that nearly three-quarters of all data requests from law enforcement and intelligence agencies to communications companies involved data less than three months old, or just over 90 days.[10] Given the significant cost of a data retention scheme on communications companies, consumers and, possibly, taxpayers, there is curiously little debate about whether a more costly two year retention period has any evidentiary basis of any kind.

7. Data retention is a direct threat to core democratic processes

A functioning, healthy democracy needs members of parliament and a media (in the broad sense, not just newspapers and broadcasters) prepared to hold governments and powerful private interests to account. In turn, politicians and the media need whistleblowers and sources who are prepared to reveal wrongdoing and provide transparency in the public interest. However, a data retention scheme makes it significantly easier, not merely for governments but for corporations and well-resourced individuals, to hunt down whistleblowers who contact public officials or journalists using telephones or unencrypted online connections. The Australian Federal Police has admitted in Senate Estimates that in hunting for whistleblowers it obtains the metadata of journalists[11] and even politicians[12] themselves. While not related to data retention directly, the Committee will itself be aware that Parliament House's CCTV system was used to identify a Department of Parliamentary Services staff member providing information to a senator (and current Committee member). There are known cases of European governments using data retention regimes established under the European Union data retention directive to hunt down whistleblowers.

Further, by requiring companies to hold metadata for a period such as two years (or even permanently, as some agencies and, apparently, some Committee members would like), it will also provide a resource for companies to subpoena information in the hunt for internal whistleblowers or as part of litigation strategies against critics and legal adversaries. It would also create a rich trove of information about activists and protesters that law enforcement and intelligence agencies have persistently targeted for surveillance, even if they engage in purely legal activities.

The threat that data retention poses to whistleblowers, journalists, politicians and anyone who seeks to hold the powerful to account is real and direct. Data retention *will* have a chilling effect on free speech and a free press, and further reduce accountability and transparency of the powerful in Australia. The government, echoing other governments around the world, has repeatedly claimed that terrorists are motivated by hatred of the

---

[10] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/docs/statistics_on_requests_for_data_under_the_data_retention_directive_en.pdf, accessed 14 Jan 2015

[11] http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;db=COMMITTEES;id=committees%2Festimate%2Fb65d6111-3180-4362-b98c-96bf25cbcb65%2F0004;query=Id%3A%22committees%2Festimate%2Fb65d6111-3180-4362-b98c-96bf25cbcb65%2F0000%22, accessed 5 Jan 2015

[12] http://www.aph.gov.au/~/media/Estimates/Live/legcon_ctte/estimates/bud_1314/ag/QoN_43-AFP.ashx, accessed 5 Jan 2015

freedoms that citizens in Western countries enjoy. If that is true, it is perverse indeed that the government should curb those very freedoms in response.

8. There is no adequate oversight of agencies

The data retention proposal raises a final issue that the Committee has, during the course of this parliament, been engaging with in its consideration of the 2014 changes to national security laws. Australia simply does not have an effective oversight mechanism for intelligence and law enforcement agencies engaged in counter-terrorism activities. To be effective, such a mechanism must be independent of government, operate in public to the extent allowed by the special nature of national security, be well-resourced, be unconstrained in what inquiries it can pursue and have the confidence of the public. Currently, there is no such mechanism. The Inspector-General of Intelligence and Security is small, poorly resourced and widely regarded as unwilling, or incapable, of offering genuine criticism of agencies within her remit. The Independent National Security Legislation Monitor – belatedly restored and appointed by the government – necessarily is confined to reviewing legislation. Parliamentary committees can be stonewalled by agencies insisting that operational matters cannot be discussed even as part of official parliamentary business. It is thus left to the Committee itself to provide effective oversight as best it can.

In its report on its inquiry into the "foreign fighters" bill last year, the Committee indicated that it wished to significantly expand its remit beyond that currently mandated by its establishing legislation, which primarily focuses on administrative matters for intelligence agencies. It has sought a role to undertake future legislative reviews — such as for preventive detention orders — as well as overseeing the specific process that national security legislation establishes (such as the process for designating certain areas prohibited). It has also sought to expand its remit to encompass the counter-terrorism activities of the Australian Federal Police (including "anything involving classified material").

The Committee should be commended for seeking to address the significant gap in our intelligence and law enforcement oversight mechanism, and should go further. Senator Faulkner, who is about to retire, had proposed a bill that (it is assumed) would have codified a larger role for the Committee in legislation. The Committee itself should carry on Senator Faulkner's work in this regard and call for legislative changes that would allow it to oversee all aspects of counter-terrorism activities as well as intelligence and security matters, and all relevant agencies within that scope, to initiate its own inquiries rather than relying on the executive to request the Committee undertake them, and to report regularly to Parliament and the public on its findings.

There would be two significant benefits from the Committee continuing to expand its role. First, by increasing independent oversight of intelligence and law enforcement agencies, it would reduce the incentives to abuse of powers that a lack of effective oversight provides. Any government agency, no matter what its purpose, will tend to abuse its powers and misallocate resources if it knows it will not have to be held accountable for its actions. By strengthening its oversight of intelligence and law enforcement agencies, the Committee will in fact be aiding those agencies themselves, as well as taxpayers.

Second, by addressing the gap in our intelligence and law enforcement oversight arrangements, the Committee will provide greater confidence to the electorate that the often draconian powers wielded by agencies such as ASIO and the AFP in relation to counter-

terrorism and crime-fighting are not being abused, and that potential abuse is more likely to be identified. It will end the current "just trust us" era of counter-terrorism, in which politicians and law enforcement and intelligence agency bureaucrats in effect work together to constantly expand the powers of government at the expense of citizens based purely on the insistence that they can be trusted with such powers. An effective oversight mechanism will reduce the need for such acts of faith, because there will be greater evidence to the public that agencies will be held to account for their actions.