Data Retention

A submission to the Parliamentary Joint Committee on Intelligence and Security

Mark Newton - 18 January 2015

Introduction

Since at least 2007, but probably before, representatives of the intelligence and law enforcement community within the Attorney-Generals Department (AGD) have been attempting to cause the Parliament of Australia to pass legislation for the mandatory retention of telecommunications data by Carriers and Carriage Service Providers.

They have steadfastly pushed this policy even though they don't seem to know what data they want, who should be able to access it, or what they should be able to do with it.

They have presented the same policy options regardless of the ideological alignment of the Government of the day or the individual who occupies the Attorney-General's office, meaning that Australian electors are denied the opportunity to choose between alternatives by casting their votes: No matter who wins an election, the bureaucrats within ASIO, the Australian Federal Police (AFP), and the various State police forces have retained their jobs and promulgated the same views. The fact that we are dealing with this issue in the way we are is profoundly anti-democratic: The term for countries where police write laws and Parliament simply does what it's told is, "Police state."

Of course, AGD hasn't acted alone. There has been a coordinated international effort among law enforcement agencies to enact and harmonise data retention laws (to the extent that they even talk about it at international conferences — There is no secret about the way they are trying to subvert democratically imposed checks and balances).

The European Union attempted mandatory data retention, causing several EU member states to pass national laws in its support. These laws were more recently neutered by decisions from their courts, on the grounds that privacy of communication is a fundamental right, and that law enforcement organisations had not been able to demonstrate that the theoretical advantages to the community of data retention outweighed the corresponding intimate violations imposed on individuals by police force surveillance.

The United States simply pursued data retention illegally: Edward Snowden's documents show that the NSA has been intercepting, storing, interrogating and interpreting virtually all telecommunications globally for years; including various outrageously illegal programs targeted at their own citizens, which NSA leadership kept hidden by lying under oath to Congress.

Australia has proceeded more slowly, ostensibly for two main reasons.

Firstly: Our AGD bureaucrats are astonishingly incompetent. When, under Attorney-General Roxon, it became apparent to them that they needed to plead their case to win their laws, they had literally no story to tell. The discussion paper released by AGD for consideration by this committee in 2012 invested a single 4-line paragraph into the matter

of data retention, expecting everything and justifying nothing. Wisely, this Committee refused to engage, concluding that insufficient information had been provided to enable any meaningful recommendations.

Secondly: The fact that AGD was being expected to justify their requirements in the first place must have come as an cataclysmic shock to them, because they've been able to become so accustomed to getting everything they want whenever they want it. The Telecommunications (Interception and Access) Act 1979 has been amended by the Parliament approximately every 18 months since 2001, usually upon presentation of last-minute amendment bills that have been whisked through the Parliament without any meaningful dissenting voice. Data retention is turning out differently for them, and they have such a vanishingly small concept of how to handle it that they've had the issue on the table for a decade, and they still, even after draft legislation has been produced, aren't able to define the data they actually want.

My view of the history of the policy in Australia

I first encountered data retention in Australia in 2007, under the Howard Government, when I was working for a large Australian ISP. There were various interactions between our staff and "the spooks," and whether or not we'd be interested in storing historical data on our customers was one of the matters up for informal discussion.

It wasn't possible to take it seriously at the time, because the prospect of secretly storing vast quantities of data in the manner they were suggesting was frankly laughable. To begin with, our customers would have lost their minds if they caught wind of it. But even without that consideration, why would a profit-making business take steps to spend substantial quantities of money on the storage of data that had no commercial value? The proposal reeked of indifference to the needs of business and ignorance of the operation of the internet.

Time passed, and an election was held, then in 2010 AGD presented a discussion paper which laid-out a detailed specification of the data that agencies wished to have retained, with examples of sample data, an industry background section, and a set of questions which they expected responsive carriage service providers to answer. They'd clearly done *some* homework, but their questionnaire was interwoven with the same indifference and ignorance, as if the fact that they had no idea what impact their regulatory proposals would have on businesses simply didn't matter.

The ISP I worked for wrote a response which, among other things, stipulated that there was no business reason for retaining much of the data; that the data we retained at the time was only kept for the period of time needed to produce a bill; and that the capital cost alone of storing the data specified in the AGD discussion paper to an adequate

standard of integrity and security was equivalent to about 20% of the company's revenue, and that it would therefore have driven the company out of business.

More time passed, then in 2012 AGD produced its discussion paper containing a set of proposals for reform of Australia's National Security legislation. To the best of my knowledge, AGD withheld information about the previous discussion paper and the results of its ISP consultation from PJCIS when your committee carried out the 2012 consultation.

Despite the reasonably extensive industry consultation, that discussion paper contained virtually no detail about data retention. I made a submission to your committee under that inquiry, where I made the same points I could very well make now, because in the passage of the three years since the inquiry, AGD has answered none of them.

I commend my 2012 submission to the Committee now, and urge you to read it in conjunction with this one.

Still more time passed, and another election was held, another Government changed, and the precise same policy has come back, with AGD making the same arguments even though they've been soundly demolished time and time again over the course of nearly a decade. AGD bureaucrats have been so indifferent to the change of Government that their resurrection of the policy in 2014/15 has included the same fonts and formatting as the version presented to ISPs under the previous Government in 2010. Having housetrained a new Attorney-General to the same standard as the last one, why would AGD need to change a thing?

Parts of the government's position they're prepared to talk about

AGD agencies make a series of arguments about data retention which, given the time and energy that has been spent engaging with them over the last 8 or 9 years, they *know* are false. They participate in the public debate about mass surveillance in bad faith, and are only able to keep making their points by assuming that nobody in power will mount a meaningful challenge to their dishonesty.

Let's walk through some of their major talking points:

The suggestion that they're merely asking ISPs to keep data that they're keeping anyway? False. That issue was addressed in 2007, 2010, and in the PJCIS National Security Legislation inquiry in 2012. No rational human being believes that AGD is asking ISPs to behave like that; The proposal on the table right now is that ISPs would be required to construct data they currently don't keep because they have no conceivable business need for it.

The Government's insistence that web browsing history would not be kept? False. The specifications provided to ISPs in 2010 and published by ZDNet on August 28th 2014, the brief specification tabled in Parliament in response to Senator Scott Ludlum's questions in 2012, the other discussion paper and specification sent to ISPs and leaked to Fairfax on August 27th 2014, and the actual text of the bill *all* include source *and destination* data for Internet communications.

The Government claims that the new Section 187A exempts web browsing history from the data retention regime; that claim is even more ridiculous, and I will address its faults in specific detail below.

AGD declares that data retention is merely giving the Government access to capabilities they used to have in the days of voice communications, which they have since lost as networks have modernized. This issue has been exceedingly well canvassed, and their contention is also false: Modern telecommunications networks provide access to substantially more data than voice networks ever did. For example: The "cell ID" specification in AGD's 2010 and 2014 specifications ***would provide law enforcement with 24x7 near-real-time high-resolution location data for every Australian with a mobile phone,*** a surveillance capability which they have never possessed (and would, one hopes, not receive if they ever asked for it).

AGD ignores the results of its own consultations with ISPs when it states that it won't cost carriers very much to comply. In the 2010 consultation, Telstra expressed the volume of data they would be required to maintain as a function of the number of semi-trailer loads of documents they'd accumulate per day, and the submission from the ISP I worked for estimated the required capital expenditure for the storage infrastructure alone at 20% of annual revenue, and further estimated that it'd cost a similar amount per annum in operational expenditure to ensure that the data was secure, backed-up, and maintained in adherence to the requirements of the Commonwealth's Protective Security Manual and Information Security Manual.

AGD also claims that the EU and UK have implemented data retention, and they are merely harmonising us with them. That assertion is also false: In 2014, the European Court of Justice said that mass data retention is not justified by the purpose of protecting national security and addressing serious crime, despite the legitimacy of that aim, and struck down the national laws that had already been passed in a small number of EU member states who had been able to legislate for data retention without violating their own constitutions. The key point is that balance is required: Placing every citizen in a nation permanently under the watchful eyes of the police is an extremist position, it is simply not balanced.

Even if the EUCJ had concluded differently, the bill before this Committee now distinguishes itself from theirs by the fact that is contains nothing which limits the use of

data to national security or serious crime. The proposal before us enables an unspecified list of government agencies decided by the Minister, who may or may not be law enforcement agencies, to use retained data for any purpose whatsoever. For the Government to claim otherwise is nothing more than a continuation of the dishonest bad faith with which AGD has approached this issue since the beginning.

Parts of the Government's position they aren't prepared to talk about

It is also instructive to consider the parts of the Government's position they aren't speaking about.

For example, it is completely clear that concentrating large amounts of personal data inside ISPs represents a massive security risk. The issue has been presented to AGD during their 2010 consultations, and I raised it with your Committee in my submission in 2012, when I said:

> And despite all the expense, all the waste, and all the new security vulnerabilities, we'd never be able to seriously trust it, because we'd never be able to be sure that an attacker hadn't already compromised its security measures and used their unauthorized access to insert or alter fraudulent evidence; or that a political party hadn't authorized ASIO to slurp up all the communications and financial records of their political opponents. Don't just think about how it'll be used, think also about how it'll be misused, with 1980's Queensland as the benchmark.

ISPs are nothing more or less than companies, and, just like any other company, they suffer security breaches. Australia has no mandatory breach notification law, so when an ISP's trove of retained data is exfiltrated by a hacker from Frankston, Penrith, Russia or China, the Australian citizens identified by that data would never know.

The various data set specifications produced by AGD over the years represent *enormously* attractive targets: detailed financial information, minute-by-minute logs of every Australian's physical location, records of everyone's communications. All the reasons that AGD provides for wanting that data also apply to actors who are even less trustworthy than the AFP.

So one would expect that a Government department interested in the national security of Australian citizens would have something to say about a proposal which would put the private data of every Australian citizen at risk of exfiltration by bad actors. But they don't: The Government doesn't seem to have disagreed with the reasonable and realistic proposition that mandatory data retention will harm our national security, it simply chooses not to engage with the topic at all.

AGD has also avoided any discussion of the extreme waste involved in this proposal. They're expecting ISPs to maintain records for law enforcement purposes on 23 million Australians without regard to whether any of those people are going to be party to a criminal investigation in the next two years. That is an inordinately expensive proposition, something they'd never suggest if they had to pay for it themselves out of tax revenues, even if the Parliament permitted such a gross violation of civil liberties in the first place. Expecting ISPs to maintain the data on their behalf represents a massive cost-shift, imposing the wastefulness of government inefficiency onto the shoulders of the private sector. This issue has come up time and time again, and AGD never acknowledges it.

Another major issue they are refusing to talk about concerns the matter of who will have access to this data. AGD claims that the proposed amendments will limit access to Telecommunications Data to law enforcement organizations and the Australian Customs Service. But the text of the actual legislation also allows the Minister to unilaterally add to the list, so there's no way of knowing who will ever have warrantless access to it.

But that's almost irrelevant when you consider that the text of the legislation places no limits on who can access data with a court order under civil discovery or subpoena. Communications Minister Malcolm Turnbull addressed the matter somewhat ham-fistedly recently, when he said that the legislation would only permit law enforcement organisations to access retained data in furtherance of criminal investigations, so police wouldn't be able to use it to aid rights holders in copyright infringement cases. That argument was completely nonsensical, given that the proposed law would enable copyright rights holders to gain access to the data without the police's help, by the method of making an application in a suitable court for discovery as part of a civil copyright infringement complaint.

Not just them: Anyone. The draft legislation currently before us draws no distinction between the data retention trove and any other collection of documents held by a business. In addition to the operational cost of maintaining the store of data in the first place, ISPs would have the additional burden of spending their lives running around servicing discovery in relation to cases that have nothing to do with them.

There is also no reference to privacy in the proposal, and the Government simply refuses to acknowledge that the issue is even worth engaging. The vast majority of ISPs in Australia are small enough to remain below the thresholds required for protection of private data under the Privacy Act, yet the Bill contains no stipulations at all about how the data should be collected, how it can be used, where it can be stored, and what ISPs are permitted to do with it outside the purpose for which it has been collected. And yet this data constitutes the most extreme example imaginable of "Personally Identifying Information", being specifically intended for the frictionless mass identification of individuals.

It is inexplicable that such privacy-sensitive legislation can be proposed in this day and age without any reference whatsoever to the Privacy Act 1998 or the Australian Privacy Principles regulated by the Office of the Australian Information Commissioner.

To provide but one example of the contemptuous indifference to national security which AGD has shown in relation to data retention: There is nothing in the Bill to prevent an Australian ISP from choosing a cheap-and-cheerful hosting provider in China for the storage of Australian telecommunications data. ISPs need the retained data, and will not care if its storage is reliable, they'll just be looking for "cheap:" If a cloud operator in another jurisdiction is $1 per terabyte cheaper than the competition, why wouldn't ISPs choose it? If they're building their own infrastructure and Huaweii, a Chinese company banned from supplying to NBNCo for AGD-originated security concerns, is 5% cheaper, wouldn't ISPs be foolish to buy from anyone else?

These are all issues which have been part of the public debate for years, which AGD has simply refused to address. AGD has gone to the extent of writing draft legislation and has *still* refused to address them. It's extraordinary that we could have come as far as we have on this issue without (for example) addressing the unprecedented security vulnerabilities ISPs and AGD will be inflicting on Australian citizens and businesses against their will, and with the government maintaining a misleading position on the issue of who will have access to retained data.

Section 187A

Since Attorney General Brandis' disastrous Walkley Award winning interview with David Speers on Sky News, in which the Attorney-General stumbled helplessly and haplessly around the metadata issue to the ongoing hilarity of his internet audience, it has been apparent that the Government is extremely eager to promulgate a view that web browsing history will not be included in the mandatory data retention regime.

Their position is desperate nonsense.

The data set specification distributed to ISPs in a 2014 confidential discussion paper leaked to Fairfax and published in the Sydney Morning Herald on August 27th includes a requirement to retain, "Information necessary to identify the destination of a communication," which includes, "the identifier(s) allocated to an account, service and/or device to which a communication is sent or attempted to be sent."

In relation to a communication which is a request for a web page, "the identifier(s) allocated to a … service … to which a communication is sent or attempted to be sent," necessarily includes the web page's URL.

The specification also stipulates, "Information necessary to trace and identify the source of a communication," including, "identifier(s) allocated to an account, service and/or device from which a communication is sent or attempted to be sent."

In relation to a communication which is the content of a web page, "the identifier(s) allocated to a … service … from which a communication is sent," also necessarily includes the web page's URL.

The text of the bill itself is frankly bizarre, and has clearly been written by someone who has no knowledge of what the internet is or how it works.

Section 187A(4)(c) says, "This section does not require a service provider to keep, or cause to be kept: information that: states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider; and was obtained by the service provider only as a result of providing the service."

That construction is nonsensical: ***All* internet traffic "states an address to which a communication was sent on the internet, from a telecommunications device, using an internet access service provided by the service provider, obtained by the service provider only as a result of providing the service."**

If the footnote next to 187A(4)(b)(ii) is in any way meaningful, it must surely exempt the retention of all data about all internet traffic. Every internet session meets the definitions in 187A(4)(b), that's the way the TCP/IP internet protocol suite actually works.

Does nobody within AGD know what the Internet is?

An email message contains "an address to which a communication was sent on the internet, … using an internet access service provided by the service provider." So if we are to believe the footnote in 187A(4)(b), ISPs will never need to retain data about email.

What about Voice over IP phone calls? They are vectored to "an address to which a communication was sent on the internet, … using an internet access service provided by the service provider." So if 187A means what the Government says it means, law enforcement isn't interested in data relating to phone calls anymore.

Service by service, you can perform the same analysis: If it meaningfully excludes web browsing history, the actual text of 187A(4)(b) also exempts literally everything else on the internet from retention.

Is that the Government's position? *Really?*

To an extent, it hardly matters: Telstra has a well-established track record of yielding web browsing history data to any police force that asks for it, without a warrant, in the absence of any law forcing them to do so. What good is a mere law anyway, when a telco can be a law unto itself? If the Bill was anything more than an AGD land-grab, it would regulate that kind of conduct out of existence. Yet it's strangely silent about the practice.

The argument mounted by the Government, that the data retention legislation they have proposed does not capture web browsing history, is ridiculous contemptible nonsense. It is only possible to come to that conclusion if you have literally no idea whatsoever about what the internet is, how it works, and what Telecommunications Data is — Just like Senator George Brandis, and just like the uninformed and unqualified person who drafted section 187A(4) in response to his embarrassment on Sky News.

Why are we doing this?

In my submission to your Committee's 2012 consultation, I quoted AFP Assistant Commissioner Neil Gaughan in an interview with ZDNet, who said, "… it's really hard to say that 250,000 requests for telecommunications data didn't lead to a significant number of prosecutions." In response to Mr. Gaughan's contention, I posed the simple question, "Why is it hard? Why isn't the AFP maintaining statistics about that information?"

It isn't an unreasonable question. Since the mandatory data retention topic first came to my attention in 2007, police forces have *always* said that the reason they want the data is to aid criminal investigations. So it's rational to expect that they would have at least *some* records to show that their existing access to telecommunications data is helpful for securing convictions, or that the absence of mandatory data retention is somehow inhibiting their function as police.

It turns out that they have no such data — They've never had it, despite the fact that they've been asked for it at various intervals since at least 2007.

That leads us to the next question I asked in my 2012 submission to JPCIS: "How can they come before this Committee requesting additional powers without providing any quantitative evidence that their existing powers are insufficient? It seems all we're really left with is `ticking time bomb' movie-plot scenarios…" made up out of the imagination of our law enforcement community, presented as hypotheticals.

Are AGD's agencies truly so administratively inept that they are unable to maintain statistics about their own telecommunications data wins and losses, even while they're appearing before Parliament to say they want more of it?

Law enforcement agencies already have the ability, under the existing Telecommunications (Interception and Access) Act 1979, to require carriage service

providers to retain telecommunications data in relation to persons of interest. If there is an active criminal investigation in progress, existing tools provide for very rapid and effective assistance from telcos.

What the existing law doesn't permit, and what AGD agencies clearly desire, is "fishing expeditions," where they can maintain permanent surveillance on every man, woman and child in the country, and retrospectively search for aberrant behaviour.

"Fishing expeditions" are the only capability they gain under mandatory data retention that they don't already have under the existing regime of targeted telecommunications data surveillance.

A maxim often attributed to Cardinal Richelieu: "Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre" ("If you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him.")

Under permanent surveillance, everyone is guilty of something. We enjoy the rule of law in Australia, which, among other things, places limits on the behaviour of government agents to enforce fairness and prevent abuses. Placing 23 million Australians under the kind of permanent surveillance which tells the government where they've been, to whom they have been talking, and what they've been spending their money on is as far from the rule of law as I can imagine.

It's more reminiscent of dystopian futures you read about in Science Fiction novels. Or a higher tech version of what the police did in East Germany before the fall of the Berlin Wall. As an Australian citizen who will never commit a crime, it is most definitely *not* how I expect my own Government to treat me.

Summary

Since Edward Snowden's revelations about illegal mass surveillance carried out by the National Security Agency (NSA) in the United States, a debate has raged world-wide over limits to the intrusiveness Governments should be able to impose on free citizens.

Apart from stepping in occasionally to label Snowden as a traitor, the Australian Government has remained largely aloof from that debate, refusing to engage. Meanwhile the debate has continued regardless, without the Government's participation, and a consensus has been forming.

Governments should not have *carte blanche* access to free citizens' lives.

Now we have a proposal in front of us to mandate in Australia precisely the kind of conduct which Snowden revealed was being carried out illegally by the United States. The Government expects to be able to enact the proposal into law even as the debate about its legitimacy continues below. It is clear that AGD does not believe that the concerns, beliefs and arguments of the governed are in any way relevant: Its position has remained the same no matter how the political winds have blown, no matter where the ongoing privacy debate has shifted.

That arrogance has no place in our democracy. It is unreasonable for AGD to sit above we citizens as a ruler, ignoring consultation, ploughing ahead regardless. AGD serves the Government and the electorate, not the other way around.

I am incredibly concerned by the overreach this proposal represents. Even if it was the same as the US, UK or EU proposals (and it isn't!), it's different in character because the US, the UK and the EU all have bills of rights which citizens can use to curb governmental abuse. In contrast, Australians have no defence whatsoever in relation to abusive behaviour by its law enforcement bodies. Our only recourse is in Royal Commissions into corruption, sometimes decades after the fact.

And we know they are abusive. Every state Police Force in Australia has had a judicial inquiry or Royal Commission into corruption inside of my lifetime, and it's realistic to expect that there will be many more. Last year Fairfax revealed that NSW Police's Internal Affairs group lied to magistrates to obtain warrants for the installation of listening devices, so we already know that police cannot be trusted with surveillance powers: there will always be bad actors abusing the law, and we need checks, balances and safeguards to protect ourselves from them.

Warrants, lawful protections from obnoxious and unnecessary surveillance, and review by public oversight, checks, and balances are our safeguards. Police aren't supposed to do whatever they want without being authorised by the Parliament *and* overseen individually by a judge. Police who behave in excess of their lawful authority are supposed to be rooted-out and sanctioned.

The proposal before us now contains no safeguards against abuse: It's open slather. It expects that carriage service providers will collect all data all the time and provide it to everyone, with no warrants, no justification, no pause for judicial reflection, and no *ex post facto* review.

Let us remember that the AFP that is demanding more telecommunications data right now is the very same AFP that detained Mohammad Haneef *due to telecommunications data suspicions arising from the origin of his mobile phone's SIM card*. The AFP has never adequately accounted for itself in relation to that travesty of justice, no legislation has ever been passed to prevent it from happening again, and Commissioner Mick Keelty didn't lose his job over his completely deficient lack of judgement. So here we have an actual

example of the attempted destruction of a human being's life over misuse of telecommunications data evidence, and it doesn't fit AGD's narrative, so the police is struck dumb and silent.

If this Bill becomes law, there will be many more Haneefs, many more innocent people placed in Kafkaesque scenarios where they are expected to prove innocence because a computer algorithm has asserted suspicion, or because, as in the Haneef case, police have once more looked for evidence to justify their own suspicions instead of evidence to determine truth. Police forces who have spent the 2000's neglecting or refusing to learn how telecommunications work in the 21st century will continue to make mistakes, to the outrageous detriment of their citizen victims; and there will be no realistic or proportionate recourse.

I urge the Committee to recommend abandonment of this incomplete, rushed, and badly engineered bill. In its place, we need *meaningful* consultation from AGD, a root-and-branch evaluation of our current surveillance laws, and a gap analysis to identify where they should be changed to assist law enforcement, while also protecting citizens from inevitable law enforcement abusiveness.