Submission to the Parliamentary Joint Committee on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill

Brian Ridgway

10 January 2015

Contents

1. Introduction

Over the past several years Australian parliaments have considered how legislation should enable law enforcement and security agencies to do their work in a rapidly changing communications environment. At a time when there is a heightened awareness of threats from terrorism, it is important that legislators carefully consider any new laws intended to make us safer and not pass laws that threaten freedoms that up to now we have taken for granted.

In 2012 the previous administration sought views from the PJCIS regarding data retention, with proposals relying heavily on the EU Data Retention Directive as an exemplar. Since that time, the Court of Justice of the EU has found data retention undermines the right to privacy[1] and therefore attempting to base Australian legislation using EU law as a template no longer presents such a convincing case.

In the 2012 enquiry many respondents had serious concerns regarding data retention. These concerns have not diminished; indeed with the better understanding today of the pervasiveness of metadata, these concerns are heightened.

In 2015 we are again considering mandating metadata retention with a Bill[2] that I believe in its current form is essentially flawed.

- Blanket mandatory data retention will fundamentally change the relationship between the government and the citizen.
- The vulnerabilities introduced by data retention will damage the state of our national security and will make Australians MORE vulnerable and LESS secure.
- In adopting data retention, Australia will be ignoring the fundamental rights to privacy and data protection as exemplified by the recent ruling of the Court of Justice of the EU.
- The Bill does not adequately test the notion of proportionality in sacrificing the privacy of citizens in order to better detect criminality.
- It will be expensive and ineffective.

I am concerned because this Bill will mandate Carriage Service Providers to retain customer metadata for a period of 2 years. This will require them to create, collect and store metadata *on all customers* and make it available in near real-time to Law Enforcement Agencies (LEAs) and other bodies nominated by the A-G. This metadata is in excess of what communications providers currently store for commercial purposes.

Targeted communications surveillance, undertaken by LEAs via warrant, is a necessary and effective weapon in fighting serious crime including terrorism. However unwarranted blanket data retention is fraught with dangers and represents a step change in powers that citizens would be required cede to government.

The proposals outlined in the Bill lack proportionality and if enacted will sacrifice the privacy of all Australians for no commensurate and demonstrable improvement in the capacity to detect serious offences. The capture of metadata would in theory enable automated profiling of each citizen with a chilling effect on democracy and perceived freedom of expression. Parallels with Jeremy Bentham's Panopticon[3] are all too real. We risk sleepwalking into a surveillance society.

There is a lack of clarity in the oversight and management of the retained data and indeed the metadata itself is not even defined but left to be prescribed by regulation.

Far from making us safer, data retention will make us more vulnerable. The Bill as currently drafted will give rise to many unintended consequences.

2. It's only metadata, it's not content

The average person will generate a significant amount of metadata each day which reveals a lot about their private lives[4]. A bit like the front of an envelope analogy?

To give you an idea of how fatuous this distinction is, the embarrassing contents of your medical records are "content" and require a warrant, but the fact that you placed a call to a GP clinic on Monday, were emailed by a pathology lab on Wednesday, Googled for pharmacies near work, and then spent the next three days trying to Skype ex-girlfriends, is metadata – and doesn't need a warrant.[5]

With the proposed retention period of 2 years, the metadata will become a honeypot for civil litigants who may seek court orders. This could include family law and commercial disputes.

It has even been suggested (PwC questionnaire to Communications Alliance 24 Dec 2014) that CSPs could make commercial use of the metadata they collect[6].

The UN General Assembly 2014 report 'Promotion and protection of human rights and fundamental freedoms while countering terrorism' [7] makes this observation (s8.53):

> *By combining and aggregating information derived from communications data, it is possible to identify an individual's location, associations and activities (see A/HRC/23/40, para. 15). In the absence of special safeguards, there is virtually no secret dimension of a person's private life that would withstand close metadata analysis. Automated data-mining thus has a particularly corrosive effect on privacy.*

3. Citizens not suspects

Mandatory blanket data retention is massive invasion of privacy and if enacted *will fundamentally change the relationship between government and the citizen*. It will have a chilling effect on democracy. We will all become suspects not citizens.[8]

The idea that the government is entitled to watch all of us is fundamentally wrong. It is neither necessary nor proportionate in handling the challenges posed by terrorism and serious crime and I believe constitutes an unacceptable incursion into the civil liberties of each and every Australian.

The Bill makes no provision for the exception of professional privilege so that metadata associated with:

- lawyers and their clients
- doctors and their patients
- journalists and their contacts
- Members of Parliament and their correspondents

will be able to be collected, accessed and analyzed along with everything else.

The use of the UK's RIPA law by police to intercept journalists' phone records illustrates the problems of overreach that poorly drafted law can produce[9].

The Law Council of Australia does not support mandatory data retention[10].

4. Security

At present there are around 600 Carriage Service Providers (including ISPs and telcos) operating in Australia. The regime of data retention proposed by the Bill, with CSPs creating and maintaining their own individual databases, with the consequent lack of uniform security and vetting procedures, will inevitably result in the data being compromised at some point. It has been suggested that for cost reasons some CSPs may be compelled store the captured metadata on cloud services hosted overseas thus compounding the problem.

As evidenced by many recent well publicised examples, security breaches of this kind can have disastrous and unforeseen consequences.

Any Australian with a digital footprint (that's just about all of us) will potentially be at risk of attack from hostile groups or foreign nations. This Bill will create multiple targets for criminals to exploit stored metadata to undertake identity fraud, blackmail or just create chaos.

The vulnerabilities introduced by data retention will damage the state of our national security and will make Australians MORE vulnerable and LESS secure.

5. Effectiveness

Those who wish to circumvent the proposed law have the means to evade detection and will do so in increasing numbers if the Bill becomes law. This will inevitably result in reduced efficacy for targeted surveillance. As the Communications Alliance submission to the

committee states:

> "*A recent search of the Apple Store, for example, revealed no fewer than 267 secure messaging applications on offer – each of which is readily obtainable and potentially able to remove the user from the reach of the proposed data retention regime.*"

I understand that it is proposed that public WiFi hotspots will be exempted from the regulations thus further emasculating this ill-conceived legislation.

The US's Privacy and Civil Liberties Oversight Board found that there is little evidence that the metadata program has made the US safer[11].

The Bill assumes that all CSPs will be able to undertake the complex task of designing dynamic systems to retain a changing set of communications metadata, the details of which can be modified at any time by regulatory order. I believe most CSPs will be of the view that this will entail considerable ongoing effort (not being part of their core business) and come at a significant cost. Those drafting the Bill have given insufficient weight to this issue.

6. Data retention in the EU

In April 2014, the EU's Court of Justice (CJEU) threw out a scheme equivalent to that proposed here, noting that metadata;

> "*...may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environment*."

Most EU countries with the exception of the UK have or are in the process of changing national laws[12] to reflect this judgement. European policy makers will need to think twice before proposing any data retention or mass surveillance program in the future. (Laws recently passed in the UK expanding the use of data retention run the real risk of failing to comply with the 2002 EU privacy directive and have yet to be tested).

Australia is travelling in the opposite direction.

7. Surveillance tax

The government has indicated that they are prepared to recompense CSPs for a proportion of costs incurred in meeting the requirements of the Bill. Taxpayers will pick up the tab for this. Remaining costs will be borne by ISPs and telcos who will pass this on to consumers. In the popular mind this will be dubbed the Surveillance Tax when added to their monthly bill.

8. PJCIS Hearings

As I understand it the Joint Committee on Intelligence and Security have been given until 27 February 2015 to report on the Bill. At its first public session on 17 December 2014, the A-G's department who is responsible for the passage of the Bill was still unable to provide a meaningful definition of the metadata to be captured by ISPs and telcos, without which no substantive estimates can be made regarding cost[13].

It is not clear whether either definitions or costing will be forthcoming before the JCIS is due to report at the end of February. How then will parliament be able to make an informed decision?

During evidence to the committee most of Australia's law enforcement agencies were unable to say how many times phone and web data has been used to prevent serious crimes or terrorist attacks, or how many convictions resulted from requests[14].

The Bill proposes that the definition of metadata would be by regulatory instrument. This is vague and dangerous, with mission creep embedded in its mission statement. It is not good law.

9. Responsibility of parliament

When considering introducing laws which restrict freedoms in the name of national security, it is important that politicians do not pass knee-jerk legislation which they mistakenly believe will help the nation defend itself against terrorism and serious crime.

There are many laws already on the statue book which give LEAs the power to undertake targeted surveillance in pursuit of wrongdoers; there is little evidence to suggest that increasing the size of the haystack will result in the discovery of more needles.

Parliament needs to better test the question of proportionality before Australia embarks on a regime that will greatly erode the privacy of all Australians, introduce security vulnerabilities and impose significant costs.

The UN General Assembly 2014 report 'Promotion and protection of human rights and fundamental freedoms while countering terrorism' [15]makes this observation (s7.51):

> *The related principle of proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest.*

I do not see that a convincing case has been made to show that this balance has been struck.

Recent surveys have shown that 80% of respondents 'disapprove of the Australian Government being able to access their phone and internet records without a warrant'.[16] I do

not believe that, once acquainted with the facts, the great proportion of the Australian electorate will accept the unwarranted mass surveillance implicit in this Bill.

Brian Ridgway

10. References

1 https://www.accessnow.org/blog/2015/01/07/leaked-european-parliament-long-awaited-legal-study-on-data-retention

2 http://www.zdnet.com/au/mandatory-data-retention-legislation-hits-the-australian-parliament-7000035221/

3 http://en.wikipedia.org/wiki/Panopticon

4 The Guardian guide to metadata

5 http://www.theguardian.com/commentisfree/2014/aug/06/you-want-my-metadata-george-brandis-get-a-warrant

6 http://www.theregister.co.uk/2014/12/25/christmas_eve_email_asked_oz_telcos_for_metadata_retention_costs_by_jan_9th

7 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement

8 https://www.citizensnotsuspects.org.au/wp-content/uploads/2014/11/EFA-MDR-briefing-paper-141103.pdf

9 http://www.theguardian.com/uk-news/2014/oct/05/mps-police-ripa-powers-snoop-journalists

10 http://www.lawcouncil.asn.au/lawcouncil/images/LCA-PDF/mediaReleases/1429_--_Law_Council_of_Australia_does_not_support_mandatory_data_retention_proposal.pdf

11 http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf

12 https://www.openrightsgroup.org/assets/files/pdfs/reports/Data_Retention_status_EU_Dec_2014.pdf

13 http://www.crikey.com.au/2014/12/17/data-retention-hearings-off-to-nonsensical-start/

14 http://www.theguardian.com/world/2014/dec/29/metadata-most-australian-police-forces-cant-say-how-many-times-it-has-been-used-to-prevent

15 http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement

16 http://essentialvision.com.au/government-access-to-phone-and-internet-records