Submission to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014

For Information: The Honourable Member for Richmond, Justine Elliot MP

To Whom It May Concern:

Dear Sir/Ma'am,

Key concerns about a mandatory data retention scheme

Communications surveillance may only be justified when it is prescribed by law, **necessary** to achieve a legitimate aim, and **proportionate** to the aim pursued.

So is the government's proposed data retention legislation necessary?

The government has not made a compelling case as to the necessity of a mandatory data retention scheme. The primary justification put forward for this legislation is that communications data is a critical element in law enforcement and intelligence investigations and that telcos and ISPs are retaining less communications data due to changing business models.

Nonetheless, this is not a sufficient justification for an indiscriminate, society-wide mandatory data retention scheme. Law enforcement and intelligence agencies already have broad surveillance powers, including a new power introduced in 2012 giving these agencies the ability to issue *Data Preservation Notices* that compel telcos and ISPs to retain all information about persons of interest (including the content of communications) for three months. Unlike what is being proposed here, these powers provide an appropriate, targeted mechanism for data to be retained but have to date been barely used?

Is the scheme proportionate?

An indiscriminate, society-wide mandatory data retention regime would represent a massive invasion of the privacy and security of all Australians. One of the reasons the European Union's Court of Justice (CJEU) gave for ruling an equivalent scheme invalid in April 2014 was its incompatibility with individual rights, in particular privacy and the protection of personal data, primarily due to its indiscriminate nature.

The mass, indiscriminate invasion of the privacy of all Australians and the subversion of the principle of the presumption of innocence that the government's proposal would represent is simply not proportionate to the alleged benefits that the scheme would bring, especially as there are already existing powers available that will achieve many of the same benefits. In the Efficacy section below we

examine some of the claims about the effectiveness of mandatory data retention schemes.

Stand against 'mandatory data retention'

In iiNet's view, we should not be forced to collect, store or match personal information on behalf of third parties – our only obligation is to retain the information necessary to provide, maintain and bill for services. iiNet **does not** keep any web browsing history or download records, for example.
Last week the Attorney General, George Brandis said the government is now actively considering a data retention regime that could impact on anyone who uses the Internet in this country.

What exactly is proposed?

We don't know for sure; the Attorney-General's Department and various law enforcement agencies has floated at least three different suggestions over the past few years, including:
1. Limited, routine metadata that carriers normally collect for phone billing purposes.
2. A middle ground that indicates metadata on all communications, but with the metadata processed to remove the content.
3. A documented specification from government that details every bit of metadata generated by phone or online communications.
We're confused by the contradictory comments and I expect that our policy makers are, too. We have a formal briefing paper from the Attorney General's department (provided to us in March 2010) which we will focus on rather than media reports and ad hoc comments.
Law enforcement agencies (like ASIO and Federal and State Police) are proposing private companies, like iiNet, should keep ongoing and very detailed records of customers' telephone and online activity. We're not talking targeted surveillance of individuals suspected of a crime, we're talking about the wholesale collection and storage of data on your online, digital and telephone activity. These records are euphemistically labelled 'metadata' – and could include the unfiltered records of your browsing, updates, movements and phone calls, which can be readily matched to the identities in your customer account.
We don't think this 'police state' approach is a good idea, so we're fighting moves by the Australian Government to introduce legislation that would force us to collect and store your personal information.
At the end of this month, iiNet will front a Senate Committee reviewing telecommunications laws concerning interception and access to communications data or metadata, which could include introducing mandatory surveillance and data retention on the communications activities of the entire Australian population. Our statement to the Committee is summarised, in part below.
Metadata, what is it?
Metadata is information generated as you use technology. It's generated by your computer, tablet, phone, games console, smart-watch, some cars and even digital photo frames. The telecommunications data collected often contains personal and

content-specific details, as well as transactional information about the user, the device and activities taking place, including:

- The content of posts
- The content associated with web pages
- The people and organisations you associate with
- Your Internet activity, including pages you visit and when
- User data and possibly user login details with auto-fill features
- Your IP address and Internet Service Provider (like iiNet)
- Device hardware details, operating system and browser version
- Cookies and cached data from websites
- Date and time you called somebody
- Locations – like where you last accessed your email, browsed the net or made a call.

Should I really be worried?

The data collected can be incredibly sensitive – it can reveal who your friends are, where you go and what websites you visit. Indeed, it may even tell more than the content of a phone call or an email. Recent research from Stanford University showed that when this data analysed may create a revealing profile of a person's life including medical conditions, political and religious views, friends and associations.

Police say *"If you have nothing to hide, then you shouldn't be worried"*. Personally I think that if you follow that dubious logic, we'd all be walking around naked. It's not about being worried, or wanting to 'hide' anything. It's about the right to decide what you keep private and what you allow to be shared. YOU should be the one to make that call, and that decision should stick until a warrant or something similar is issued to law enforcement agencies to seize your information.

Not convinced? Then we suggest you check out the startling website based on information collected on German politician Malte Spitz by Deutsche Telekom over just six months. Zeit Online combined this geo-location data with information relating to his life as a politician, such as Twitter feeds, blog entries and websites, all of which is all freely available on the Internet. It's really worth a look and illustrates just how informative and personally invasive metadata can be – it is truly scary stuff.

Experts in the US have some equally frightening things to say about metadata. According to NSA General Counsel Stewart Baker, *"…metadata absolutely tells you everything about somebody's life."* General Michael Hayden, former director of the NSA and the CIA, called Baker's comment *"absolutely correct,"* and frighteningly asserted, *"We kill people based on metadata."*

If it helps catch crooks, what's the problem?

Australia already has systems in place to help catch crooks.

The Telecommunications (Interception and Access) Act specifies the circumstances in which interception of customer communications is lawful and when it is permitted for telecommunications companies to disclose communications data.

The focus of this data retention proposal is not crooks; it's the 23 million law-abiding men, women and children that will go about their daily lives without ever bothering law enforcement. Those 23 million customers include my 93-year-old

mum and my 12-year-old niece. We don't believe that is either necessary or proportionate for law enforcement.
We've seen no evidence that justifies surveilling inoffensive customers on the chance that, two years later, some evidence might help an investigation. It's the equivalent of collecting and storing every single haystack in the country, indexing and filing all the straws, keeping them safe for two years, just in case there's a needle, somewhere. We don't know if there's a needle, but there might be.
I say forget spying on my mother and niece and get on with chasing the crooks.

What will this all cost?

It is hard to measure exactly what this will all cost, but we expect that collecting and keeping every customer's 'metadata' would require the construction of many new data centres, each storing petabytes (that's 1 billion megabytes!) of information at a cost of tens or hundreds of millions of dollars. There is no suggestion that the government would pay these costs, so our customers will be expected to pick up these costs in the form of a new surveillance tax.
If they need someone to process the full set of metadata down to metadata-minus-content, then there is a significant cost to process the collected metadata and redact it. (Imagine a lot of people with thick black markers, blotting out the content – just like the government does with some Freedom-of-Information requests).
The Government must also consider the privacy implications if Internet providers are to be compelled to collect data on Australians. The vast amount of data stored would prove to be an appealing target for hackers all around the world – creating a risk of information and identity theft in the event that storage of the data is breached.
It's not right. It's not Australian, we don't support it.
To demonstrate the true cost of data retention, we created a useful infographic. Although it highlights the costs to iiNet, just one Internet Service Provider, imagine if this was applied to ALL ISPs!

See more at: http://blog.iinet.net.au/protecting-your-privacy/#sthash.b2gTRqP3.dpuf

My greatest gripe is **Cost:**

It has been estimated that a mandatory data retention regime would add at least $5 per month to every internet connection account, unless the government chooses to fund such a regime, which would cost many hundreds of millions of dollars to set up and to operate.

Given that different telcos and ISPs currently retain different types of data for differing lengths of time, as determined by their individual business models, the implementation costs of this scheme will vary significantly, and will impact smaller and leaner operators harder than the bigger operators. Telstra, for example, as well as having a much greater capacity to absorb these costs, also already collects and retains (it is understood) much of the data the government is seeking for significant periods of time. Other providers, such as iiNet, retain much less data and in many cases delete that data quite quickly as they have no business reason to store it. These providers will therefore be required to create and store data

that they currently do not.

This scheme will therefore have significantly adverse effects on competition with the telco and ISP markets and may force some smaller operators out of business as well as creating new barriers to entry to the market. A joint submission by the Australian Mobile Telecommunications Association and Communications Alliance to the 2012 inquiry by the PJCIS estimated the cost of the scheme proposed by the then Government to be between $100 million for basic data capture and $500–700 million with IP addresses included. iiNet's upper estimate was $400 million.

The result, of course, will be higher prices for businesses and consumers.

Security:

We have just signed on to a 'free trade agreement' with China who are pro-cyber-attack upon the free world. The creation of massive databases of highly personal information will act as "honeypots" which will be actively targeted by malicious individuals and organised crime syndicates. In addition, the risk of inadvertent data breaches is very real – the Federal Police and the Immigration Department have both had serious inadvertent data breaches recently – as is misuse of the data by disgruntled or compromised employees.

Companies forced to retain data will seek to use the cheapest data hosting available to minimise the cost of compliance. As Steve Dalby, Chief Regulatory Officer from iiNet said last year, the cheapest data hosting available at the moment is in China. This raises the additional threat of the data being compromised by the intelligence agencies of other countries.

The question is therefore not whether this information will be compromised, but rather when and how. Any such data leak could have serious implications for the affected individuals, particularly for vulnerable people such as victims of stalking and other forms of harassment, as well as for public officials such as judges and even politicians.

The government's proposals therefore represent a real threat to the privacy and security of all Australians. So much for our free trade agreement!

Use of data in civil litigation:

The data retained under this scheme will be available to be used in civil litigation by court-issued subpoena. This means it will be able to be used in copyright infringement cases, and particularly as the data is to be retained for such a long duration, will likely lead to a great deal more "speculative invoicing" (or "copyright trolling" – see the EFA's article about this issue here). It will also potentially be used in unfair dismissal cases and other civil cases wherever a litigant can convince a judge that the data *may* be relevant to the case.

Urgency:

The issue that the Attorney-General's Department is seeking to address is by its very nature a long-term one. There is simply no justification for it to be dealt with in the expedited manner that the government is using. Rather it should be subject to lengthy and considered scrutiny by the parliament. The tactic of using the largely confected idea of a 'terror emergency' to force this legislation through parliament quickly is deeply disingenuous.

"This handy submission guide has been put together with our friends from Electronic Frontiers Australia (EFA), who GetUp have partnered with on this campaign."

In conclusion, freedom is a value that all should share and not be subjected by intervening government all in the name of 'terrorism'. If government was to educate and rehabilitate offenders leaning towards terrorism, the cost to the majority of the population would be minimal.
Communication is no longer secure with government's intervention to the private sector, but to make it policy is abhorrent to our freedom as a society.

Sincerely,

Roger Graf

18th January 2015