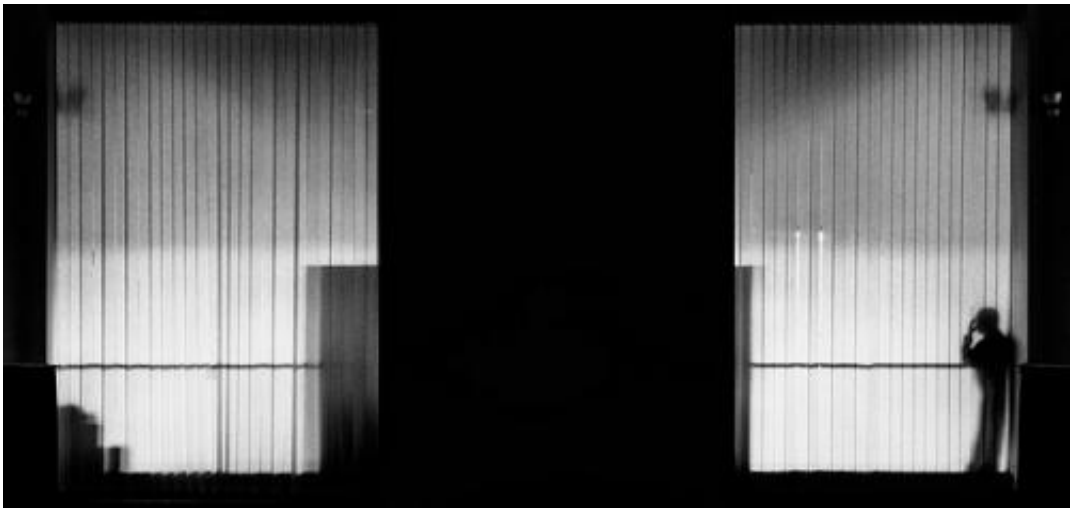
Individual privacy versus digital driftnets

March 30 2015, by Suelette Dreyfus And Shanton Chang



How safe is your metadata once it's been collected and stored? Credit: Flickr/David Melchor Diaz, CC BY-NC-ND

The great irony of the Abbott government's plan enforce the mandatory data retention legislation is that while this is being done to make us safer, in fact it creates new data security risks for us all.

While much of the debate has been dominated by the anti-surveillance vs protection camps, with attention paid to journalistic field, the more obvious data security risks have been largely ignored by the two major parties, with the Senate passing the legislation with minimal scrutiny.

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 – now passed by both Houses – will force

telecommunications companies and internet service providers (ISPs) to gather and store for two years an enormous amount of data about their customers' communications, such as whom you call on your phone, how long you talk for and a close approximation of your location when you make that call.

The intelligence and security agencies have told the public they need this information so they can trawl the information looking for the bad guys.

Yet the huge data set this proposed law will create is in itself a giant security risk, even for the innocent and boring, so it is also a security paradox.

The principle of privacy

The approach demanded by this Bill is completely at odds with the recently passed Australian Privacy Principles which say, in brief, don't gather more data than you need to, don't keep it longer than necessary and destroy the data when you no longer need it.

As an example, Principle 3 says:

[…] an organisation, may only collect this information where it is reasonably necessary for the organisation's functions or activities.

Further the Principles require organisations to ensure "the security of personal information it holds".

But the sheer amount of data that will need to be collected, stored and secured will be a security risk, making companies collecting the data ripe pickings for hackers who specialise in identity theft.

The data covered should not be downplayed as just metadata – it's your

life in a nutshell. If you call a suicide hotline or a obstetrician, anyone going through that data can conclude a great deal without actually hearing the conversation's content. It is exactly the kind of data that identity theft rackets look for, now stored for two years.

Why, then, are they doing this?

The only people pushing for this law are a small set of government agencies and departments. They already have extraordinary powers, and received yet more just recently, such as the controversial "Special Intelligence Operations" provisions which makes it legal for ASIO officers to break the law, including lying to Parliament and the courts.

Even the normally docile Inspector-General of Intelligence and Security has flagged concerns about these expanded powers last year.

No hard evidence has been provided as to why any these new powers are actually necessary, including the data retention proposal.

It's important to remember that these law enforcement agencies already have the power to access telecommunications data, issue data preservation notices and seek a warrant to intercept communications.

The amendments for journalists are an improvement but often organisations have a suspicion of who has leaked information to the media. There is no warrant required for following the electronic breadcrumbs from the door of the alleged source, only from the journalist's end. Thus the newly imposed protection has only limited value.

This legislation will have a profound effect on the very fabric of our free and open society, despite the welcomed amendments. Journalists across the country will see sources dry up.

Whistleblowers who reveal stories that really do matter to average Australians – like the live-baiting of greyhounds or political corruption – will think twice before contacting the media because all phone records will be kept for two years.

The legislation will also likely have a negative impact on other relationships that rely on trust and confidentiality such as lawyer/client and doctor/patient or even politician/constituent.

Data retention elsewhere

There are 11 countries in the European Union that have data retention schemes and have still managed to make sure there is some independent oversight, often by a judge.

In fact, Europe shows us that data retention schemes are moving in the opposite direction to Australia. Schemes in Austria, Bulgaria, the Czech Republic and Cyprus have been ruled unconstitutional.

The UK legislation – held up as a model here and justification for why we need one too – is in fact under legal challenge. The Court of Justice of the European Union shot down the Data Retention Directive.

Germany abandoned its data retention scheme. A German study showed no discernible improvement in solving crimes when the scheme was in place.

The European countries that still do retain data typically do so for only six to 12 months – much less than the two years proposed in Australia's legislation. The less data kept, the lower the security risk to the citizenry. The reality is, privacy is something we are losing bit by bit, so painlessly that we don't even see it.

What do IT experts think about this?

The amendments do not set a standard for encryption, and good security requires more than encryption. The amendments also fail to address the issue of off-shore storage of data.

Those who work in the telecommunications industry, or are responsible for information security would tell you that this poses a real risk for not just society, but individual users.

There is also a common misconception that someone is going to sit in front of a computer and trawl through line by line of your phone calls or other meaningless numbers.

In fact, data analytics tools (which is the science of examining often disparate raw data to draw conclusions about a phenomenon) can be built to automate most of this trawling, and your identity can be cobbled together very quickly and from a wide variety of sources (all of which will now be in common repositories).

Creating a situation where the data is stored for such a long time, you would hope ISPs have a crack team of IT experts to defend our data.

Yet, Australia continues to face a shortage of IT skills. The Australian IT Industry which includes our key ISPs, continue to rely on foreign supply of these skills.

This is unavoidable as long as low numbers of Australian students choose to take up IT programs post-secondary education. This situation potentially places our well of data in the hands of non-Australians, which is an interesting proposition to increase national security.

At every new crossroad in law where privacy, security and technology

collide, we must ask: is this new law reasonable, necessary and proportionate? That case has not been made here, particularly for all the complex internet data.

Dr Suelette Dreyfus is participating in the IQ2 public debate in Sydney on Tuesday March 31, 2015, on the topic Only The Wicked Need Fear Government Spying.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation