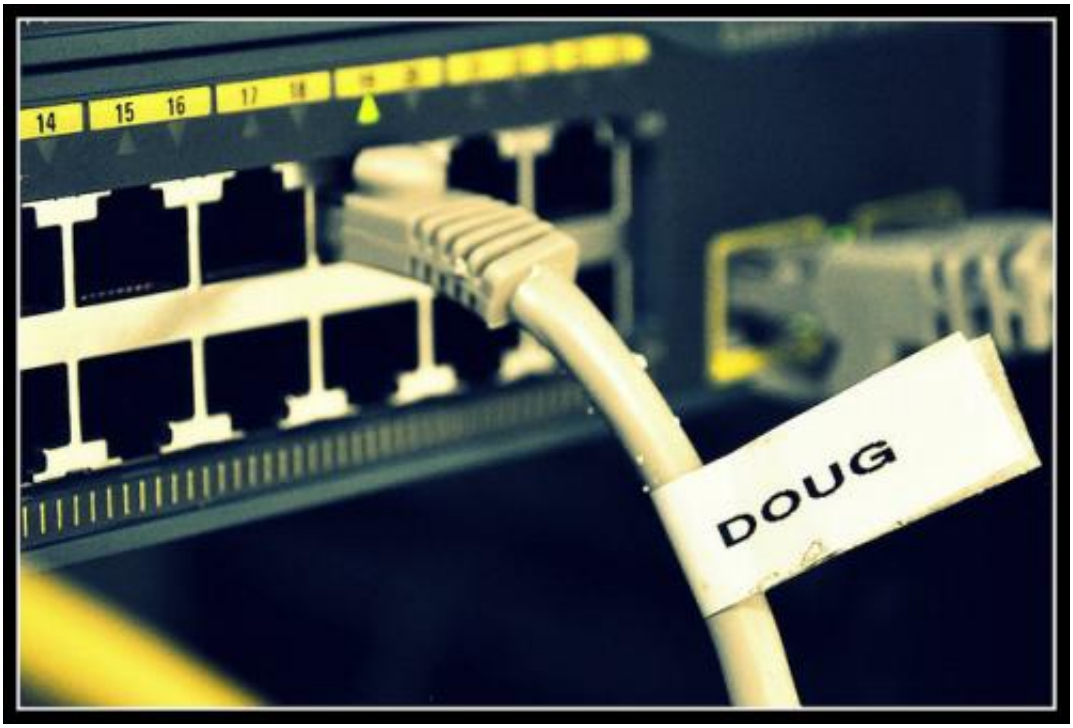
It's not 'what' but 'who' you connect with in metadata retention

February 24 2015, by Luke Heemsbergen



Who is Doug talking to, and will Australia's proposed metadata retention scheme be able to find out? Credit: Flickr/Doug, CC BY-NC-ND

The purpose and implementation of the Australian government's proposed metadata retention scheme is making less sense as political pressure mounts to get the legislation passed. So what's going on?

The bill, as written, suggests it can be easy for criminals to "opt out" of

data collection, while the remainder of Australians still have their personal communications spied on, retained for two years and kept in commercial data centres at taxpayers' expense.

The Australian Greens senator Scott Ludlam recently raised a number of such concerns about the bill which has already met opposition from privacy advocates.

But the bill's worth as a tool to specifically fight terrorism, or any other serious crime, seems dubious if potential terrorists and criminals in Australia can easily "opt out" of having their data retained simply by choosing any internet messaging service where the persons operating the service do not own or operate "in Australia, infrastructure that enables" that service.

So what does that mean for the apps commonly used on smartphones today?

Whatsapp, the popular mobile messaging app with 700 million users, around 10% of which come from the Middle East, or Viber, a similar app with 20 million users in Pakistan alone, would both be excluded from data retention. These are some of the apps that the UK's prime minister David Cameron recently mused about baning in the UK.

According to answers given by Australian Attorney General's (AG) department staff during the Senate Legal and Constitutional Affairs Reference Committee, the "in Australia" provision also means that even Google's web-based Gmail service is excluded from data retention.

So what does the bill call for?

With all the reports of what the bill leaves out and doesn't do, no one seems to acknowledge what is actually in the draft bill, and how that

language might affect policing, government and privacy. So what is at play?

One possible explanation is that Australia is carrying out its obligations as part of the "five eyes" network of English speaking intelligence partners. The logic here is that it makes economic and political sense to have Australian internet service providers (ISPs) such as Telstra and iiNet retain what originates in their infrastructure rather than have the US's National Security Agency (NSA) collect it.

A more plausible explanation is that, contrary to the PM's politiking, the data to be retained is not valued by the Australian government for its national security or anti-child abuse value.

Instead, Australians are to be spied on for data that will become valuable for other state functions including the expanded reach of civil litigation. The expanded value considers normal policing, civil subpoenas and even copyright disputes.

A look inside the bill

The Australian government is not explicitly interested in the internet protocol (IP) addresses that you visit. The bill in its current form states in section 187A that the government:

[…] 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.

In more detail, the helpful "explanatory memorandum" codifies that:

Under proposed paragraph 187A(4)(b), the retention obligation is explicitly expressed to exclude the retention of destination web address

identifiers, such as destination internet Protocol (IP) addresses or uniform resource locators (URLs).

So what are we talking about then?

It's all about the destination

What the government does seem to be after is "destination" data that basically amounts to an assortment of dummy variables that help identify you, and who you are communicating with.

Instead of IP address or web pages, it is interested in retaining email accounts, Skype handles and phone numbers, etc. for the connections you have made.

The government's "destination" is in many ways more invasive than IP addresses or web URLs alone. For instance, think about how each person in Australia connects to the IP address 69.63.176.13. That's the IP for Facebook.com, and is physically located in the US.

Retaining the metadata of time spent at that address would not produce much actionable intelligence on you or the other 8 million Australians who browse Facebook each day. Nor would it be all that invasive to privacy.

"Destination" data is different. "Destination" data seeks to capture who, specifically, you're spending time with online; who is the destination that you are messaging through email, Skype or possibly even Facebook's real-time apps and services?

Think of it this way: two "destinations" pass data through the same communications service at a series of very specific times, again, again and again. No other two "destinations" share this unique pattern of time

and connection.

The government's definition of "destination" is multiple click here, search for "destination"), but we can isolate a key phrase:

This information can then assist with determining the subscribers who sent or received relevant communications.

That is to say, who you're talking to online, not where you went.

Analysing how these "destinations" link together with other metadata (geo-location, device type/operating system, etc.) allows the government – or anyone else who snoops in on the retained data – to predict, for instance, that these communications were yours, and whether you targeted them to, let's say, your spouse, or an "old friend" across town. And whether you meet up with that person from time to time. And where. And for how long.

Geolocation data alone is incredibly powerful when we all carry smartphone and other devices that connect to the internet in our pockets. People are just starting to learn how powerful this type of metadata is.

Retaining all of that metadata provides an incredible amount of information for civil litagants that can ask for it through a subpoena. As an former iiNet lawyer wrote:

The Data Retention Bill does not impose any limitation on access to the retained data by other legal avenues. This means there's nothing stopping your ex-husband, your employer, the tax office or a bank using a subpoena to get access to that data if it is relevant to a court case.

All this data also creates a very valuable target for hackers, including "adversarial intelligence agencies" trying to infiltrate your identity,

ransom you for your secrets, or run some form of economic espionage.

Can we trust Australian service providers can keep all the data safe once they've accumulated two years worth of intimate connections for each Australian who uses any sort of telecommunications device?

Sadly, recent security breaches at companies as diverse as Apple, Target, and the latest heist from "100 banks and other financial institutions in 30 nations" suggest otherwise.

The flawed explanations of what good the bill does, what privacy risks it creates and the reality of how our retained data will be used, offers many red flags on why this legislation should be reconsidered.

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

Source: The Conversation

Citation: It's not 'what' but 'who' you connect with in metadata retention (2015, February 24) retrieved 5 July 2024 from https://phys.org/news/2015-02-metadata-retention.html