What metadata does the government want about you?

August 28 2014, by Philip Branch

The government wants your movements online to be retained by ISPs and other companies. Credit: Flickr/Envato , CC BY

With the leaking of a discussion paper on telecommunications data retention, we are at last starting to get some clarity as to just what metadata the Abbott government is likely to ask telecommunications companies, internet servce providers (ISPs) and others involved in communications services to store.

The paper is written to be "technology neutral" but the intention seems to be to ensure that the same information available from interception of traditional telephony is available from internet-based communications.

Essentially the law enforcement agencies want two types of "telecommunications data" (the term they use for metadata). First they want information about account owners ("subscribers") and second they want information sufficient to let them link traffic back to that subscriber.

Account owner information includes obvious data such as names and address, but also related information such as billing data, contact information and the like. They want to be able to find out who the user of a particular account is.

There is nothing new here. This is the same kind of information they have had access to for a very long time.

The second point is information that can enable captured traffic to be linked to that account. This is the most interesting part of the document.

Internet and telephone communication are not the same

In traditional telephony the link between identity and traffic is straightforward. The parties to a communication can be found from their telephone numbers. Telephone numbers do not change and are linked to a specific subscriber.

Unfortunately for the law enforcement authorities, in internet-based communication the story is much more complicated.

Internet communication is built upon a technology called packet switched networking. When we send an email, look up a web page or use an IP phone, our communication is split into discrete chunks of data called packets.

These packets are then transmitted between end points based on source and destination addresses contained within a header in each packet. This approach to networking allows great resilience and flexibility.

But for law enforcement authorities it creates all sorts of challenges. In particular there is no identifier that plays the same role in the internet as a telephone number.

No fixed address online

The nearest is the IP address. Unfortunately, the link between identity and IP address is quite weak. IP addresses are not fixed. The IP address used by someone today may well be used by someone else tomorrow.

IP addresses may actually change during the course of communication. A technology (Network Address Translation) may substitute one IP address for another. Just knowing an IP address does not give the same information as a telephone number.

It seems to be the goal of the paper to make sure that telcos, ISPs and other service providers store sufficient information so that it provides the same information for someone on the internet as with telephone numbers.

Traffic might be observed going to and from a terrorist website. The law enforcement authorities would like to know who is accessing that website.

They see that the IP address of the person accessing the website belongs to a particular ISP. They go to the ISP and ask who was using that IP address at the time the website was accessed.

The government's document aims to make sure the ISP retains enough

metadata so that they can answer that question.

What the government really wants

So does it succeed? It seems the goal of the document is solely to provide the same sort of data that can be obtained from traditional telephony. But there are a few concerns.

The first is that the author wants upload and download volumes to be recorded. This might simply be to see if the account is active but it could also be used as a basis for investigating illegal downloads.

The second is that although it is written to be technology neutral, it is obvious that the law enforcement authorities' surveillance systems and equipment are shaped by telephony, rather than the internet.

Reading the document, one can almost feel sorry for the author as he or she tries to map internet based systems onto traditional telephony. With the internet the distinction between metadata and data is much less clear.

It may well be that how interception is done, what metadata is accessed and, most importantly, who can request it needs to be revisited.

Provided by The Conversation