How will data retention laws cope with the Internet of Things?

Philip Branch

One of the many things that is troubling about the current Australian government's metadata retention proposals is how rooted in the past they are, which could make them obsolete before they even come into force.

The Telecommunications Interception Act was first enacted in 1979, when telephony was the only widespread and available communications service. Updates to the act have really only been at the edges, keeping in place the assumption that communications is essentially telephony with a few additional services.

However, as has been pointed out many times before, modern communications is much more than telephony. Modern communications is used more and in many different ways by far more of us than was the case with the simple telephone. Yet interception is still built on a telephony model, most apparently in the continued distinction between data and metadata.

Lawful interception of telephony distinguishes between "intercept related information" (metadata) and "call content" (the actual voice conversation). In telephony, metadata consists of the parties to a call, the duration of the call, any call forwarding and perhaps (in mobile telephony) the location of the parties.

In telephony, distinguishing between metadata and call content made sense. In modern communications it does not. Attempting to identify the boundary between what is and what is not metadata in the modern communications environment leads to all manner of contradictions and confusion.

For example, when it was suggested that compulsorily retained metadata might include websites that were visited, there was such an uproar that the legislation will now explicitly exclude such information. But why should it? Why is it necessary to distinguish between different types of metadata? The answer is that some metadata is more sensitive than others.

The problem is that developments in modern communication make the concept of metadata meaningless. There is really only data, some of which is of greater or lesser sensitivity depending on the circumstances. New technologies have made the contradictions inherent in basing legislation on a telephony model increasingly apparent. Worryingly, emerging technologies risk making the contradictions even more absurd than they already are.

For example, there is a great deal of interest in massively increasing the number of devices connected to the internet. This is the so-called "Internet of Things" (IoT) or "Internet of Everything". Cisco believes that by 2020 there may be 50 billion "things" connected to the internet. Proponents envision that any object in your house or place of work may well have a wireless transmitter, receiver, IP address and be able to communicate autonomously with other systems.

IoT has great potential in industrial applications, particularly manufacturing but also in domestic applications. The possibilities range from the mundane to the bizarre.

A mundane example is that your refrigerator might note that you are getting low on yogurt and order in some more. A slightly bizarre possibility is that your toaster might decide you are not eating enough toast to warrant keeping it and decide to sell itself. A vaguely alarming proposal is that your toilet might do some analysis of what you flush and let you know if you should see a doctor.

Whether these things happen, and whether they should happen, is a discussion for another time. But if the number and variety of devices connected to the internet massively increases, how will legislation relating to compulsory retention of metadata be applied to it? New technology developments may make the distinction between metadata and data even more of a problem than it is now.

A fundamental question is what constitutes metadata in these circumstances? Often the message sent from one device will be for another to switch on or off. The metadata may well be little more than the message.

Will ISPs be required to keep metadata, whatever it is defined to be, relating to all these devices? iiNet believes the cost of retaining all metadata for a single person per year will be around $130.

Unfortunately we don't yet know what metadata is to be kept, but have been assured that not all metadata will be, so the cost will probably not be quite that high. But presumably there will be some cost, and if the number of end devices increases by several orders of magnitude, it is likely to be significant.

Metadata can already provide deep insights into how we live our lives. Stores of such information are likely to be an attractive hacking target. What new threats to privacy will metadata from our household objects create? And what new exclusions, similar to that for web browsing, will need to be enacted?

Interception legislation needs to be brought up to date. A good place to start will be to dispense with the outdated distinction between metadata and data.

As noted earlier, in modern communications there is only data, some of which is more sensitive than others. That should be reflected in the legislation. Otherwise the revised legislation risks being out of date not long after it is released.

Dr. Philip Branch