Metadata and the law: What your smartphone really says about you

March 3 2014, by Philip Branch

The move to mobile technology has opened up a wealth of metadata, but that information goes deeper than you may first think. The Fuji street shooter/Flickr, CC BY-NC-ND

Metadata related to lawful interception has been in the news a bit lately. You may have seen last week the Australian Federal Police (AFP) called for more access to electronic metadata as a Senate committee evaluates Australian mass surveillance laws.

Probably most people understand that lawful interception (wiretapping or phonetapping) has moved beyond connecting alligator clips to a phone line, but "metadata" might be a bit of a mystery.

If you have ever wondered why you need to provide identifying information such as a driver's licence when you purchase a new phone, "metadata" is a big part of the answer.

So what is metadata?

Metadata is information about communication, rather than the content of the communication itself.

We are all familiar with metadata. It consists of such things as telephone numbers, email addresses, webpage addresses and the like. It is what we see when we look at our telephone bill.

The reason it is in the news now is that modern telecommunications has caused an explosion in new forms of metadata.

When telecommunications mainly consisted of voice and perhaps short message service (SMS) the actual content of the communications was rarely collected. Capturing, recording, storing and listening to voice conversations was expensive and, at least during the early stages of an investigation, probably of limited value.

What was useful though was information about the call – information as to who was talking to whom and how often, enabled investigators to construct a model of the relationships between those of interest.

Maybe at a later stage conversations would be recorded, but usually intercepts requested by the authorities delivered information about the call, rather than the call itself – in other words, the "metadata".

Mobile metadata

Even before smartphones and the internet, metadata from the mobile phone system was surprisingly rich. Metadata could provide information as to whether the call was forwarded and where it was forwarded to, whether or not it was answered, and so on.

Such information is invaluable in building up a model of relationships. But not only did the phone network provide information about the participants to a call, it could also provide approximate information about where the call was made.

Since mobile phones are connected to the network via nearby base stations usually located only a few kilometres away, metadata reporting which basestation the handset is attached to gives location information accurate to a few kilometres.

Also, since the phone is connected to a basestation whenever it is switched on, the phone can provide continuous location information regardless as to whether or not calls are made.

This was the situation with the widely used 2G mobile phone networks which were deployed in Australia during the early 90s and which are still in use. However, telecommunications has moved on a great deal in the past few decades with many more possibilities for investigators.

All the metadata available in the 2G network is available along with much more, but of particular importance is that the way mobile devices are used has changed. Most obviously, mobile devices are used to access internet services.

Enter mobile internet

Mobile internet has been both a blessing and a curse for investigators. Smartphones are used for many more purposes than voice only

telephones.

Generally, people use a smartphone much more than they used older types of telephones. Consequently, many new forms of metadata have become available. Email addresses, websites visited, files downloaded all present many new opportunities for investigators to gather metadata.

Not only is material downloaded, but a considerable amount of material is also uploaded.

Pictures, videos, social media updates all provide metadata that could be of use in an investigation. For example, images captured on a smartphone will, unless steps are taken to remove it, contain GPS location information accurate to within a few metres.

Other metadata that might be of interest includes when the image was created, who created it and the device it was created on. Metadata might even be added, perhaps unwittingly, when people tag images with comments.

The proliferation of metadata options has caused problems for investigators too. Any online service that enables communication can be used to thwart interception. For example, most online games contain some messaging feature, and there is no reason why this cannot be used as a way of exchanging messages.

Webmail drafts are another example. In this approach people who wish to communicate do so by sharing an email address from a webmail provider and write drafts of emails which are saved and read by participants, but are never sent. The metadata of interest here is not just the email address, but the identities of those who accessed it.

Integrating metadata from potentially multiple sources is also a

challenge. A draft webmail communication as described might involve metadata from the telephone company, an internet service provider (ISP) and the webmail provider.

Because there are so many new possibilities and difficulties regarding metadata the whole area of lawful interception and surveillance has come under frequent review the past decade. There was a proposal last year by the Australian government – since shelved – that all ISPs should store for two years all communications that contained potentially useful metadata.

There are many issues to consider, from both law enforcement and privacy perspectives. No doubt we will hear a lot more about metadata in the next few years.

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

Provided by The Conversation

Citation: Metadata and the law: What your smartphone really says about you (2014, March 3) retrieved 23 May 2024 from https://phys.org/news/2014-03-metadata-law-smartphone.html