Think your metadata is only visible to national security agencies? Think again

August 5 2019, by Damien Manuel

Credit: CC0 Public Domain

It was bound to happen, and it did. Poorly crafted legislation – designed to allow national security agencies to collect information with the aim of protecting Australians from terrorists—is now reportedly being exploited

by a range of different government agencies for other purposes.

It has been widely reported that the Veterinary Surgeons Board of WA, Victorian Fisheries, Liverpool City Council, and the Australian Sports Anti-Doping Authority are among the entities that have requested access to metadata.

Under the Telecommunications (Interception and Access) Act 1979, only agencies tasked with enforcing criminal law are entitled to access metadata from telecommunications companies.

Metadata is the information recorded by the telco when you make a call or use the internet. It can include information such as where you are, whom you called or texted, how long you talked for, how frequently you called or texted someone, what services you used, what websites you visited and when, and much more besides.

Under the legislation there are 22 criminal law enforcement agencies that can legally access these metadata. They include the federal police, state police forces, the Australian Criminal Intelligence Commission, federal and state police integrity commissions, state anti-corruption bodies, and parts of the Australian Border Force.

The federal home affairs minister also has the power to declare other agencies as "enforcement agencies" under the law.

Why is data being accessed?

Generally, enforcement agencies are entitled to access metadata if it is either given to them voluntarily, or if they issue a formal request for information they believe is required to perform their duty.

The definition of an enforcement agency was narrowed in 2015, at the

same time the federal government introduced the controversial mandatory data retention framework, which requires telcos to retain customers' metadata for at least two years.

Before the definition was tightened, an estimated 80 different agencies were covered by the previous laws. They included not just criminal and national security investigators, but also a wide range of agencies pursuing financial matters such as unpaid fines or taxes.

Since 2015, however, most of those agencies found themselves excluded by the new definition of an enforcement agency, but could use a range of laws that still grant powers to request metadata directly. One example is Section 20 of the New South Wales Fair Trading Act 1987. According to the submission made by the Australian Communications Alliance to the Parliamentary Joint Committee on Intelligence and Security, 60 federal and state agencies have sought access to metadata via this mechanism.

What is metadata anyway?

The information contained in metadata was infamously described by former Attorney-General George Brandis as the "material on the front of the envelope" (rather than the contents of the letter itself). But in reality it is much, much more.

Of course, metadata can be useful to help telcos improve their services, by revealing peak calling times or popular locations on the network. But you can also think of metadata as a digital breadcrumb trail that each of us leaves in our wake as we go about our lives.

It can provide enough information to establish a detailed picture of someone's life: their daily routine, relationships, interests, preferences, and behaviour. It can even reveal someone's location, to whom they have spoken, and for how long.

It seems excessive that two years' worth of someone's metadata can be kept on file and then obtained without a warrant. Although the low access threshold was called out in submissions before the law was passed, there was no public discussion of the implications for privacy and liberty.

If properly understood, the metadata access regime would not pass the pub test.

How is metadata really being used?

The federal home affairs department's 2017-18 annual report lists a range of offences for which metadata has been sought by various agencies.

The report says that information was sought in relation to a total of 23,586 criminal offences including homicides, abductions, sexual assaults, fraud, robbery and drug offences.

The report also reveals that 300,781 items of metadata were disclosed during the reporting period in total across all categories.

Law enforcement agencies have claimed that metadata helps to eliminate suspects by revealing their networks and contacts. But there is no information regarding the use of metadata by government bodies that are not officially enforcement agencies within the meaning of the data retention laws.

In simple terms, there is no central public report that outlines how all state and federal agencies are accessing and using this information.

Metadata stored is available to any enforcement body with the power (under state or federal law) to request or require the information. By

tightening its definition of "enforcement agencies" in 2015, the federal government denied many smaller agencies the right to access metadata directly, but did not prevent them from getting it via other means. As a consequence they were also excluded from supervision by the Commonwealth Ombudsman.

One interesting exception is that civil courts are prevented from obtaining metadata as evidence in civil proceedings, unless the metadata was collected and held by the telco for some purpose other than the mandatory data retention regime. Given the huge range of other authorities that can access it, this seems rather arbitrary and unfair.

So where to from here? Besides amending the law, it is also time for a wider public debate over the correct balance between our privacy and civil liberty on one hand, and our protection and national security on the other. This is especially important as we become more and more reliant on digital technology to live and work. Just imagine the privacy implications with 5G, when more personal devices are connected to the internet like your smart meter, light bulbs and toaster.

Provided by The Conversation