PHYS.ORG

Is it possible to circumvent metadata retention and retain your privacy?

March 31 2015, by Philip Branch

Many of your online activities leave a digital trace that can reveal your identity. Credit: mikael altemark/Flickr, CC BY

There has been quite a lot discussion lately on how to avoid metadata retention, particularly in the context of leaking sensitive information to journalists.

Notable examples have come from journalist Laura Tingle and, rather surprisingly, Malcolm Turnbull, who gave the impression that avoiding metadata collection was trivially easy.

Is metadata retention really that easy to avoid? If so, what is the point of the legislation? Has parliament just passed a bill for a A$400 million white elephant? Let us have a look at some of the suggestions for legally avoiding metadata collection and see how they stack up.

Third party protection?

One of Laura Tingle's suggestions is that whistleblowers use Skype to avoid metadata collection. The reasoning is that Skype communication is encrypted and the servers are located in Estonia, beyond the reach of Australian metadata collection.

Unfortunately, this suggestion confuses a number of things. It is true that the content of a Skype call is encrypted, and that the signalling to set up the call might go via servers located in countries beyond the collection capability of our intelligence agencies.

But Skype is a peer-to-peer protocol. Once the call is established, there will be a stream of packets containing the call content travelling between participants. The content of these packets might be indecipherable, but the metadata (i.e. the IP addresses) showing communication between participants may be collected and can be traced back to the identities of the participants.

Not my email

Another suggestion is to use Google's Gmail or another offshore email service provider. Communications to these email servers are encrypted, including the source and destination email addresses.

However, there are some ways in which emails that use such services might be able to identify the sender. Most of these service providers are based in the US and so come under the "Five Eyes" agreement.

Under this agreement the US, UK, NZ, Canada and Australia share intelligence data. Also, if the recipient's email server is located in Australia, once the email is delivered to it, the source email address will be visible and can be collected.

A messaging application favoured by Mr Turnbull is Wickr. Using this is a much better suggestion. Wickr messages are sent to a server and then delivered to the recipient when they log in. The metadata captured for both the sender and receiver will only show that there has been communication with the Wickr server. There is no metadata directly linking the recipient and the sender.

Wickr also has some impressive features that secure it against the possibility of being compelled to hand over data from logfiles. But it too is not perfectly secure.

If the recipient is online when the message is sent, they will receive the message a very short time afterwards. An investigator with access to the metadata could get a good idea of who the sender was by finding a correlation between who sent messages to the Wickr server just before the recipient received them.

From WLAN to VPN

So how might metadata retention be avoided legally? As noted here, the fundamental problem is avoiding connections between your identity and the device the message is sent on, and any accounts used to send it. Using a work computer and any email address, social media handle or other identifier that is in anyway linked to the sender is not secure.

One possibility is to use a WLAN service that does not require registration, such as the Wi-Fi at your local cafe or shopping centre. The person who wishes to avoid detection takes their WLAN device to the local shopping centre and just joins it. So long as they do not have to register, they may avoid identification.

However, there are a few things to be wary of. Using WLAN access from a smart phone is probably not a good idea. At the time of purchase, a lot of identification information is supplied. The WLAN address is linked to that smart phone and might be able to be traced back to the owner.

Once again, using a device that cannot be traced to the sender would be necessary. Of course they would also have to use a secure service such as Wickr that could not be traced back to them.

Another approach might be to use a virtual private network (VPN). This will cause communications between the sender and the VPN server to be encrypted. As with Wickr, the only metadata that will be collected will show that the recipient's data came from the VPN server.

But, again, there are things to be wary of. As with email, using a VPN server that is based in one of the "Five Eyes" countries is probably not a good idea. Even if the server is overseas, the VPN provider may well retain logs of who connected and when, which might be seized by that country's law enforcement agency and, ultimately, identify the sender.

Entering the onion

A number of news organisations have a secure drop system based on Tor . Tor consists of a number of nodes within the internet through which communications is routed. It makes use of encryption techniques to ensure that communications between the nodes of Tor cannot be traced back to the source.

But again some caution is needed. Many organisations track use of Tor access and may ask awkward questions as to why the sender was using Tor around the time of a major leak. But, again, using a device that cannot be traced to the sender will make detection difficult.

So what can we make of this? Scott Ludlum may have been a little harsh when reportedly told a group of university that metadata collection might only catch the stupid criminals.

But with a little care the legislation can, at the moment, be sidestepped. However, avoidance is reliant on services and devices that cannot be traced to an individual. It is unlikely that law enforcement agencies would tolerate such a gap in their capabilities.

Perhaps we will see further legislation in this area yet.

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

Source: The Conversation

Citation: Is it possible to circumvent metadata retention and retain your privacy? (2015, March 31) retrieved 20 March 2024 from https://phys.org/news/2015-03-circumvent-metadata-retention-retain-privacy.html