GlobalResearch
Center for Research on Globalization

Australia's Surveillance State: Metadata and the Derogation of Privacy Rights

By Dr. Binoy Kampmark
Global Research, August 09, 2014
Region: Oceania
Theme: Police State & Civil Rights

It is sometimes hard to know whether those in power adopt a policy of confusion purposely, or through grand design. When it comes to the flawed policy of data retention on a mass scale, a burden that is bound to fall on telecommunications companies, the problem is most acute of all. What is to be kept? What falls within that broad term metadata?

The Australian Prime Minister, Tony Abbott, a somewhat challenged individual in twenty first century politics, is one such example. Here, dinosaur meets politician, and the result is far from pretty. It is less pretty for the fact that his Attorney-General, George Brandis, is talking another language on the same subject.

Neither seems entirely clear what the subject of metadata constitutes. For Abbott, it is a matter of dealing with "the material on the front of the envelope" while leaving the contents of the letter untouched, a crudely inaccurate analogy if ever there was one. On public channels, Brandis claims that the new proposals on mandatory data retention would require internet service providers (ISPs) to retain "metadata" for up to two years which would include "the web address" of each site visited by the individual user.

Within the Australian cabinet, some dissent has brewed over the subject. The communications minister, Malcolm Turnbull[1], is irritated for good reason – he is the one left carrying the can and mollifying ISPs over their onerous duties. He wasn't even invited to Monday's national security committee meeting.

Turnbull, in an attempt to clear the mud that had invariably slipped into the waters, suggested on Friday that metadata was a matter of difference. In his postmodern retort, a user's web browsing history would not be part of the captured mix.

> "There has been some concern expressed that the government was proposing that telcos should retain for two years a record of the websites that you visit when you're online, whether that's expressed in the form of the domain names or their IP [internet protocol] addresses – in other words, that there would be a requirement to keep a two-year record of your web browsing or web surfing history."

Turnbull then brought in the traditional card of policing data, denying that the browsing history would be the subject of retention. "What they are seeking is that the traditional phone records that are currently kept, and by some ISPs and telcos for more than two years, that is the caller, the called party – you know, I called you, time of call, duration of call…

they want them to be kept for two years."

But of course, it does not stop there. The IP address, or as Turnbull describes it, "the number that is assigned to your phone or your computer when you go online by your ISP" is to be retained.

Similar denials on the extent of data capture have also been issued by the Australian Security Intelligence Organisation (ASIO) chief David Irvine, and the Australian federal police (AFP) deputy commissioner, Andrew Colvin. While both were keen to dispel rumours that browsing histories would be captured, they dumped on the idea that warrants were required to access metadata.

As Irvine explained, metadata was already being accessed "for many years", a process that was bound to continue. Then there was the honourable, reliable office of the Inspector-General of Intelligence and Security (not, of course, a judge or an expression of the law) keeping an eye on "the way we access [metadata]."

Colvin, in an unconvincing attempt to pacify critics, attempted to draw a distinction between metadata, which can be accessed as an "initial investigative tool" and actual content. The latter required a warrant, with its judicial protections.

Australia remains virginal when it comes to matters associated with accessing metadata, with authorities totally oblivious to a scheme of rights and protections to prevent overstretch of power. Even the independent national security legislation monitor, Bret Walker SC, has suggested a warrant system.[2] By all means, store the data, but ensure some means of control when accessing it. Traditionally conservative voices from such organisations as John Roskam of the IPA[3] have also warned that, "Once it happens there is no winding this back. It gives enormous power to the government over people's privacy. The material will leak. It will be used for purposes not related to anti-terrorism."

The assumption here is that the authorities will stick to the straight and narrow, refusing to step into the realms of illegality. Sticking to such protocols of propriety is, however, impossible in an age where metadata is the guiding principle of the information age. All governments want to feast on it, and they get rather frustrated when the civil rights lobby remind them that information should not be there for the taking without just and probable cause.

The excuse, as it always tends to be, is also one of blunt pragmatism. Privacy rights, and correlative obligations to respect them, tend to be matters of nuisance to spy chiefs and figures behind the intelligence gathering apparatus. For Irvine, having a warrant for each request for metadata would see "the whole system…grind to a halt." This is patent nonsense, seeing as an intelligence service operating within the boundaries of warrants and judicial oversight is bound to be better for it. More gaps does not necessarily imply more insecurity or less freedom. It does, in fact, suggest the reverse.

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com*

Notes

[1]http://www.theguardian.com/world/2014/aug/08/asio-and-federal-police-seek-to-clear-up-confusion-over-metadata-collection

[2]http://www.abc.net.au/lateline/content/2014/s4062418.htm

[3]http://www.businessspectator.com.au/article/2014/8/8/technology/abbotts-national-security-failure

---

Articles by: **Dr. Binoy Kampmark**