THE CONVERSATION

Academic rigour, journalistic flair

The metadata report disregards a range of reports demonstrating that retention is ineffective. Flickr/r2hox, CC BY-SA

We are all suspects now thanks to Australia's data retention plans

March 2, 2015 3.23pm AEDT

Author

Bruce Baer Arnold
Assistant Professor, School of Law, University of Canberra

Australia's Parliamentary Joint Committee on Intelligence & Security (PJCIS) last week endorsed the data retention bill, which means we're all suspects now.

The Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 provides for mandatory retention by internet service providers (ISPs), phone companies and other entities of telecommunications metadata -– data that in aggregate provides a picture of our lives.

The data will be accessible by a wide range of law enforcement and other bodies, potentially extending from the Australian Security Intelligence Organisation (ASIO) and the Australian Federal Police (AFP) to your local council, the unrestrained Independent Commission Against Corruption Website (ICAC) and even the RSPCA.

Access will be without warrant. The Bill privileges bureaucratic convenience –- and political opportunism or cowardice –- over what is effective and proportionate in the prevention and prosecution of crime.

PJCIS endorsement -– presumably to be followed by enactment hot on the heels of the New South Wales state election -– is an epochal event.

It comes after a decade in which the Australian Law Council, industry, academics, civil society advocates and concerned individuals have cogently criticised proposals for retention.

Each time the Opposition of the day has expressed disquiet and a range of parliamentary committees (as late as 2014) have condemned the particular proposal as going a step too far.

This time, it seems, things are different, as the government wraps itself in the flag and the Opposition ensures that it's seen to be tough on national security. The arguments haven't changed, but a lone man with a gun in Sydney gained headlines with a terrorist flag. On that basis civil liberties disappear, and will presumably continue to erode.

What does the report say?

The 362 page report is interesting for what it doesn't say. It disregards a range of authoritative overseas national security reports, such as this high level report to the White House, demonstrating that retention is ineffective.

It also disregards warnings by analysts regarding population-scale data retention: storing data about every communication is an invitation for hacking and misuse.

It disregards the very substantial body of law in Europe, where courts have recurrently said that treating everyone as a suspect is profoundly disproportionate to the needs of law enforcement and national security. (Contrary to claims by the AFP, law enforcement in Europe hasn't collapsed when the courts have accordingly struck down retention law.)

The report does note some concerns, albeit particular recommendations can be disregarded or obfuscated by the Government. The PJCIS recommends establishment of data breach reporting –- alerting consumers when their data goes AWOL.

Given the history of data breaches involving leading phone companies and other entities such as Sony we might wonder whether breach is inevitable. The government is urged to address business criticisms by making "a substantial contribution to the upfront capital costs" facing ISPs and telcos.

The PJCIS urges the government to amend the Explanatory Memorandum to the Bill in order "to make clear that service providers are not required to keep web-browsing histories".

The Australian Securities and Investment Commission (ASIC), Australian Competition and Consumer Commission (ACCC), AFP and a slew of other agencies thus won't have warrantless access to a record of every mouse-click.

The committee also calls for restricted access regarding civil litigation, although questions remain about criminalisation of intellectual property infringements in "the war against piracy".

But who will watch the watchers?

The PJCIS notes substantive concerns by the media about freedom of expression. It appears to assume that governments will never misuse powers to track journalists and their sources.

We should, it seems, believe our watchers and disregard incidents we hear such as those in NSW where the highest executives of the police force appear to be bugging each other and where ICAC is accused of misusing its powers.

The report calls for supervision by the Commonwealth Ombudsman, meaningless unless that body is properly funded. It does not address evisceration of the Office of the Information Commissioner (whose current head is currently working from home after withdrawal of the agency's funding last year).

Presumably we are to trust a watchdog that is toothless and has been very reluctant to bite the hand that under-feeds it.

Suspicion and complicity

It is easy to blame Attorney-General George Brandis for this over-reaching national security legislation. But we should be looking at ourselves –- as a society -– and at our representatives. The silence of Bill Shorten – who appears to have forgotten that the duty of an Opposition is to oppose – is lamentable.

Liberal democracies should be confident about their values, sufficiently confident to accept that dangers -– or purported dangers -– don't necessitate creeping abandonment of civil liberties.

The government currently has strong powers to access metadata and communications content under warrant. Mandatory retention with warrantless access is an unprecedented and unnecessary step deserving robust condemnation by the PJCIS.

Failure to do so places the onus on all Australians at the next election.

Online privacy **Internet** **Online security** **Surveillance** **Metadata** **Data retention** **Metadata retention**