Australian data retention bill means mass surveillance

Mike Head
31 October 2014

The Australian data retention bill, released yesterday, reveals the underlying agenda behind the expanded “anti-terrorism” laws that the Liberal-National government is pushing through parliament with the backing of the opposition Labor Party.

The “metadata” bill provides for mass surveillance, via the storage of vast amounts of phone and on-line information, directed against the entire population.

The bill will compel all Internet providers and social media platforms to retain data for two years so that the security services can trawl through it. This will permit them to compile a detailed picture of everyone’s life, including political views, friends and associates, geographical locations and even spending habits.

That surveillance will facilitate the use of the draconian powers handed to the government and the police/intelligence agencies under two bills already passed this month. It will also feed into the global network headed by the US National Security Agency (NSA), whose spying on hundreds of millions of people around the world was exposed by NSA whistleblower Edward Snowden.

On the pretext of protecting ordinary people from Islamic State in Iraq and Syria (ISIS) and other Islamic extremists, these laws go far beyond that supposed purpose. They demonstrate the real “enemy,” as far as the political establishment is concerned, is the population itself.

When the data retention power was first proposed by the previous Labor government in 2013, it aroused such widespread opposition that Labor shelved the plan until after last year’s election. During that campaign, both major parties buried any mention of it. Now, it has been brought forward once more, against a backdrop of renewed US-led war in the Middle East and constant “terrorist” scares.

Unveiled without notice yesterday, after months of backroom discussion, the bill does not define the “metadata” that must be stored. Instead, that will be prescribed by regulations, effectively giving the government a free hand.

At their media conference, Attorney-General George Brandis and Communications Minister Malcolm Turnbull insisted that the bill did not cover the “content” of communications, nor permit the tracking of web browsing. Those assurances are meaningless, however, even though they are covered by vague clauses in the bill.

That is because the information to be kept will include everything relating to the identities of users and anyone with whom they communicate; the time and duration of every use; and the locations of mobile devices and computers involved. As intelligence commentators have explained, that is enough to amass a comprehensive dossier on anyone.

The bill’s memorandum contains a table of the data that must be stored, but then states that this is “not exhaustive.” Vodafone, a major telecommunications operator, warned that the system could extend to automated machine-to-machine devices, which include Eftpos terminals, vending machines and in-car navigational systems.

Earlier this month, iiNet, a large Internet provider, published a report disclosing the extensive information that the government wants retained. It demolished the government’s claim that the bill would only involve what the telco companies already stored. The list included “upload/download volumes” and the “identifiers” of all people communicating with a subscriber.

Yesterday, the government admitted that the data would exceed the information that the companies currently keep. Communications Minister Turnbull said the companies would get “substantial” payments to store the extra data. He refused to put a figure on the amount, but iiNet said its initial bill alone could run to $600 million.

iiNet chief regulator officer Steve Dalby warned that the industry would look for the cheapest cost option—cloud storage hosted out of China. Such cloud storage heightens privacy concerns. Narelle Clark from the Australian Communications Consumer Action Network said: “This kind of system will create a large honeypot with people who don’t have good intents and purposes.”

There will be an unprecedented expansion of government monitoring. Already, according to Australian Communications and Media Authority statistics, more than 580,000 telecommunications intercepts were permitted last year. These intercepts, by many government bodies, require no judicial warrants, simply “self-authorisation” by the agencies involved—a practice that will continue.

The government claimed that the data retention bill would limit this system by confining it to “criminal law-enforcement agencies.” Yet, this covers all the police and intelligence services. Moreover, the bill states that the list of authorised agencies can be expanded by the communications minister.

Australian Federal Police Commissioner Andrew Colvin admitted that the bill could “absolutely” help authorities target anyone who “illegally” downloads or shares content. Industry analysts said media and entertainment conglomerates would subpoena the data to sue those accused of using free or cheap download services.

In another attempt to defuse public opposition, the government declared that access to metadata was critical for criminal investigations. Turnbull told parliament that included “murder, serious sexual assaults, drug trafficking and kidnapping,” as well as “counter-terrorism, counter-espionage, cybersecurity, organised crime.”

Turnbull was seeking to divert attention from the universal character of the data storage, which is designed to track the activities of the vast majority of people. This is under conditions of increasing social unrest and political disaffection with the ruling elite’s agenda of war, austerity, widening inequality and abrogation of basic legal and democratic rights.

The data bill is the third tranche of Prime Minister Tony Abbott’s government’s “counter-terrorism” legislation. The first bill, already passed, expands the computer hacking powers of the spy agencies and imposes jail terms of up to 10 years for anyone (not just journalists) who exposes an undercover “special intelligence operation,” such as the infiltration of a political party.

The second bill, the “foreign fighters bill” parliament rubberstamped yesterday, extends the terrorism laws in many ways. Notably it outlaws “promoting” terrorism, which could include posting social media content opposing Australian involvement in the Iraq-Syria war.

The Labor Party, which unconditionally supports the war, has already assisted the government to get the first two bills passed as quickly as possible. It immediately signalled its readiness to do the same on the data retention powers.

“We believe fundamentally in the promotion of national security,” Labor leader Bill Shorten said yesterday. “The security agencies say that they need metadata retained for two years.” He declared that Labor would help “get the balance right” on “legitimate concerns for privacy” via a review by the bipartisan joint parliamentary committee on security. The same committee signed off on the first two bills, with purely token “oversight” measures.

The Greens spokesman, Senator Scott Ludlam, claimed that his party would “draw a line” at mandatory data retention. But he accepted the official rationale for the bill, telling the *Business Spectator* there were “entirely legitimate law enforcement and anti-corruption uses for metadata, and no-one really contests that.”

The Greens have a long record of posturing as critics of terrorism legislation, while voting for key measures to strengthen them. As on the Abbott government’s first two bills, their “opposition” will consist of moving cosmetic amendments to try to lend some kind of legitimacy to unvarnished police-state provisions.