World Socialist Web Site wsws.org

Reports expose Australian government’s data retention plans

Mike Head

16 October 2014

Revelations over the past week highlight the extent of the electronic surveillance already being conducted by the Australian spy agencies against the entire population, and the far-reaching scope of the “metadata retention” bill about to be unveiled by the Abbott government.

With the backing of the Labor opposition, the government is using the pretext of combatting Islamic State in Iraq and Syria (ISIS) terrorism to introduce legislation that will expand and legalise the operations conducted by the Australian agencies, as part of the US National Security Agency (NSA)-led global intelligence network, to monitor Internet communications.

As yet unseen, the proposed metadata bill will compel all Internet providers and social media platforms, including Google and Facebook, to retain immense amounts of data for two years so that the security services can trawl through it, permitting them to compile a full picture of everyone’s spending habits, political views, friends and associates and geographical locations.

This bill will be the third tranche of the Abbott government’s “counter-terrorism” legislation. Among other things, the first bill, already passed, expands the computer hacking powers of the spy agencies and imposes jail terms of up to 10 years for reporting on “special intelligence operations.”

The second bill, now before parliament, extends the terrorism laws in many ways, including to outlaw supposedly “promoting” terrorism by posting social media content that encourages opposition to Australian military operations such as the involvement in the US-led Iraq-Syria war.

Last week, iiNet, one of Australia’s major internet providers, published a report disclosing the information that the government wants retained for two years. The company said the list included material that iiNet does not currently retain, demolishing Attorney-General George Brandis’s claim, made on October 1, that the data retention law will not “involve anything beyond what the telcos do at the moment.”

According to iiNet’s paper, the categories of data on the list cover a vast array of personal information, starting with the name, date of birth, phone numbers and residential, postal and IP addresses, and billing status of each subscriber.

Also on the list is information designed to link subscribers with other government and financial records, such as: “Identification and verification data—may include passport number, Medicare number, other credit cards, rates statement.”

Other data to be stored includes “upload/download volumes,” records of the time and duration of all communications, and the “identifiers” of all people communicating, or attempting to communicate, with the subscriber.

Finally, the list requires: “Physical and logical location of device—at start of call, at end of call.” This provides a means of monitoring the geographical movements of all subscribers.

As iiNet states, the long list exposes the fraud pushed by the Australian government, together with the US and UK governments, that “metadata” is just like a letter’s envelope, giving the authorities no access to the content of communications. The stored information will be so comprehensive that the spy apparatuses can compile detailed dossiers of political targets.

The company’s paper quotes NSA general counsel Stewart Baker’s statement that “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.” iiNet concludes: “Blanket data retention is mass surveillance.”

iiNet’s paper also warns of wider privacy dangers, noting that “the retention of a vast set of personal information would likely prove to be an appealing target for hackers all around the world—creating a risk of identity theft in the event of a data breach.”

The company says government officials have provided “no guidance” on the security protocols that would apply to storing the data. “For example, will offshore cloud storage be acceptable or will the data be required to be stored in Australia?”

Further material published from the documents leaked by NSA whistleblower Edward Snowden sheds more light on how far the NSA’s Australian counterpart, the Australian Signals Directorate (ASD), and its “five eyes” partners in Canada, Britain and New Zealand are integrated into the NSA’s global surveillance.

According to a 2006 document published by the *Intercept*, the ASD has conducted secretive programs to help the NSA hack into computer networks. These programs, codenamed PAWLEYS, involve the NSA’s clandestine human intelligence capabilities (Humint), as well as “computer network access intended to obtain cryptographic information and materials.”

The document states that the Canadian, Australian, British and New Zealand agencies “all operate PAWLEYS programs and NSA collaborates with each on targets of mutual interest.”

The exact nature of the programs in which the ASD participated is unknown. Other documents published by the *Intercept*, however, show that the NSA’s “computer network exploitation” activities include working with US and foreign companies to undermine encryption systems and physically or remotely subvert computer systems.

Snowden’s previous disclosures have demonstrated the ASD’s involvement in the NSA’s surveillance of millions of Australian residents, as well as hundreds of millions of people around the world. Earlier leaks showed that, for example, the ASD offered to share “bulk, unselected, unminimised metadata” about Australians with the NSA and the other “five eyes” services in 2008. This is data in its raw state, with nothing deleted or redacted in order to protect the privacy of anyone.

Further documents published in August 2014 by the *Intercept* showed that the ASD may have fed information into the NSA’s ICREACH search engine, designed to share billions of call, email, location and chat records. Last month, Snowden described being able to access XKEYSCORE, another NSA system, which allowed NSA to mine the data of people in Australia and other “five eyes” countries.

None of these operations has anything to do with fighting small bands of terrorists, whose groups have long been known to the security agencies. These are police-state programs, directed against the population at large under conditions of deepening disaffection with the ruling elite’s program of austerity, war and erosion of fundamental legal and democratic rights.

All these mass surveillance operations, and no doubt many more, will be facilitated and expanded by the Abbott government’s data retention regime, which is being prepared with the full support of the Labor Party opposition, just as Labor has backed the first two tranches of the so-called terrorism laws.

In fact, it was the previous Labor government that first proposed the data retention legislation, then cynically deferred it until after last year’s federal election, fully aware of widespread hostility to the plan. On this front, as on the Iraq-Syria war itself, there is a completely bipartisan line-up on defying and suppressing popular opposition.