Australian Federal Police boosts data intercept capacity

Mike Head
16 December 2013

Australian Associated Press reported last week that the Australian Federal Police (AFP) is purchasing new "deep packet inspection" (DPI) technology, capable of collecting and storing vast data to track the emails and other Internet activities of millions of ordinary people. Trials of the DPI program will commence in February.

DPI allows police and intelligence agencies to monitor the addresses and subject lines of emails, and all other social media communications, as well as web-browsing habits. This covers everything that people do on-line, from phone and Skype calls to Twitter and Facebook posts. From this, it is possible to build a detailed picture of anyone's daily life, movements and associations, including their political views and activities.

America's National Security Agency (NSA) uses DPI for its immense global Internet surveillance because it can collect data in real time and capture it at 10 gigabits per second—two features requested in the AFP's tender documents. The documents also show the system must be able to "extract and store metadata," or the raw information behind messages such as phone numbers, email addresses and the dates, times, locations and duration of calls and emails.

As well as presenting an "electronic fingerprint" of people's lives, this data can be stored and extensively mined, permitting targets to be selected whose communications will be kept under surveillance, and the contents examined in depth.

The AFP told Australian Associated Press that DPI was a common "system tool" within commercial and government IT systems worldwide, and would not be connected to other telecommunications or IT networks. As the documents leaked by US whistleblower Edward Snowden show, however, the NSA and its partners, including the Australian Signals Directorate, share "bulk, unselected, unminimised metadata."

According to another report, Australia's largest telecommunications company, Telstra, recently installed advanced surveillance systems to "vacuum" the telephone calls, texts, social media messages and Internet metadata of Australians so that information can be filtered and given to intelligence and law enforcement agencies.

The equipment was purchased from Newgen Systems, the Australian supplier for Gigamon, a Silicon Valley-based IT firm. One former Newgen employee explained: "Gigamon's systems are designed to find not just a needle in a haystack, but bits of needles in many haystacks. We do that by taking all the hay, all the time. We take everything."

In a Senate committee hearing late last month, AFP Commissioner Tony Negus confirmed that the AFP collected phone and Internet data on up to four unnamed federal parliamentarians during the previous year. Asked how many MPs had been the subject of authorisation orders allowing the AFP to track their phone calls and email traffic, Negus replied: "Less than five."

If members of parliament, all part of the political establishment, are being monitored, then there is no doubt that political activists are being spied upon as well. Official data confirms that hundreds of thousands of people are under surveillance by the AFP and the state police forces, with which it works closely.

Figures reported under the Telecommunications Interception Act (TIA) show that 293,501 intercept authorisations were handed to Australia's law enforcement agencies in 2011–12, up by about 20 percent from the 243,631 in 2010–11. The vast majority of the intercepts were made by the state police forces.

These figures do not include the intelligence

apparatus, including the Australian Signals Directorate (ASD), the Australian Security Intelligence Organisation (ASIO), the domestic spy agency, and the Australian Secret Intelligence Service (ASIS), the external espionage service. They are exempt from the TIA's limited authorisation and reporting requirements.

Prime Minister Tony Abbott has sought to defend the security agencies, saying he was confident that they acted within the law and there were proper privacy safeguards in place. This is a conscious deception.

Under the TIA there are no restrictions on police and other designated government agencies gaining access to the metadata. In fact, the legislation requires the telecom and Internet companies to retain all data and hand it over to the agencies on request. No judicial warrant is required, simply an "authorisation" by any senior police or other government officer.

At an earlier Senate hearing, Commissioner Negus poured scorn on a suggestion that police agencies be required to obtain warrants before metadata can be accessed. Negus declared that this would "grind the AFP to a halt," giving an indication of how critical metadata collection has become to the police forces. Judges would have to consider thousands of police affidavits, he declared, dismissing this as "an unrealistic expectation."

The situation in Australia closely resembles that in the United States, where reports earlier this week showed that, with the support of the Obama administration, police agencies receive detailed call and location records of Americans' cell phone activity without a warrant, in violation of the US Constitution.

These reports followed revelations, based on documents from Snowden, that the NSA collects five billion records every day on cell phone users around the world, including many Americans. (See: "US tracks billions of cell phone location records daily").

In Australia, as in the US, this blanket surveillance has bipartisan support. Last year, the previous Labor government unveiled a plan to require that all metadata be stored for up to two years so that the security agencies could trawl through the data over a longer period. Public opposition ultimately forced Labor to send the proposal off to a parliamentary committee. The committee's report did not reject the proposal, but left it open for consideration once the September election was out of the way.

Far from the ongoing revelations of vast on-line surveillance by the US and its allies leading to any restriction on these activities, the spying operations are escalating in Australia, as elsewhere.

Mass surveillance, usually associated with a police-state, has deep political implications. It points to the decayed character of the façade of parliamentary democracy, and preparations for widespread repression. It also reveals a ruling class living in fear of growing discontent among broad layers of people, as economic and social conditions deteriorate.