Australian agency integrated into NSA spying operations

Peter Symonds
21 October 2013

New documents leaked by former US National Security Agency (NSA) contractor Edward Snowden and published in the *Washington Post* last week highlight the critical role of Australian agencies in the NSA's massive spying operation.

A top secret PowerPoint document revealed that the NSA is intercepting and storing personal email address books and "buddy lists" from instant messaging services as they pass around the Internet. The previously undisclosed program is immense in scope, involving the gathering of hundreds of millions of contact lists that can be later "mined" for information about targeted individuals (see: "NSA 'harvesting' electronic address books and contact lists").

The direct involvement of the Australian Signals Directorate (ASD), previously known as the Defence Signals Directorate, in the NSA operation was revealed in one PowerPoint slide detailing the collection of address books.

In just one day in January 2012, the program "harvested" 712,336 address books, of which 311,113 or more than 40 percent were provided by the "point of access" designated as DS-200B. According to the *Washington Post*, the prefix signifies "the NSA's Australian counterpart"—that is, the ASD. *Post* reporter Barton Gellman told the Fairfax press in Australia that he had been able to identify "DS" as referring to an Australian intelligence agency using "internal evidence plus one source."

Address books, the PowerPoint stated, accounted for 22 percent of the "major accesses" by the NSA's Special Source Operations. The typical daily intake corresponds to more than 250 million address books per year.

A second document, which deals with managing the vast amount of address book data collected, identifies other "points of access," including AUC (another code for Australia) as well as the prefixes—US, NZC, CAC and UKC. The United States, Australia, New Zealand, Canada and the United Kingdom form the top-level "Five Eyes" intelligence sharing network.

In addition to address books, the NSA program also collects an estimated 500,000 "buddy lists" as well as the inboxes of web-based email accounts, which "unlike address books, frequently contain content data."

Unlike the PRISM program, under which Internet companies such as Skype, Google, Facebook, YouTube, Microsoft, Yahoo, Apple provide the NSA with access to data stored on their servers, the NSA program revealed in the *Post* collects information "on the fly"—that is, as it passes through the Internet.

The collaboration of members of the "Five Eyes" is critical to NSA operations as each provides access to the undersea cables that carry the vast Internet traffic between continents. By establishing listening posts at the cable-landing sites, intelligence agencies can tap directly into the flow of electronic data.

In July, the *Washington Post* revealed that the Australian telecommunications company Telstra had signed a secret agreement in 2001 to ensure that US intelligence had access to its cables from the Asia Pacific into the US (see: "Telstra facilitates US electronic spying"). Under the arrangement, Telstra established secret listening posts in the United States staffed by American officials.

An article in the Fairfax Media on August 29 revealed that the Australian Signals Directorate in partnership with American, British and Singaporean intelligence agencies were tapping the major SEA-ME-WE-3 cable that runs from Japan, via Singapore through the Middle East to northern Europe. Australia is connected to the

cable via a link from Singapore to Perth in Western Australia.

The article explained: “Australian intelligence sources have told Fairfax Media that Singaporean intelligence co-operates with Australia in accessing and sharing communications carried by the SEA-ME-WE-3 cable which lands at Tuas on the western side of Singapore Island…The Australian Signals Directorate also accesses the SEA-ME-WE-3 cable traffic from the cable’s landing in Perth.”

A former Australian Defence intelligence officer explained that access to cable traffic “gives the five-eyes and our partners like Singapore a stranglehold on communications across the Eastern Hemisphere.” The article cited Australian intelligence sources as confirming that ASD and Singapore’s Security and Intelligence Division played “key roles” in intercepting communications traffic in Asia.

Last week’s *Washington Post* article explained that the NSA exploited non-US listening posts to circumvent the US constitution: “The NSA has not been authorised by Congress or the special intelligence court that overseas foreign surveillance to collect contact lists in bulk, and senior intelligence officials said it would be illegal to do so from facilities in the United States. The agency avoids the restrictions in the Foreign Intelligence Surveillance Act by intercepting contact lists from access points ‘all over the world’, one official said.”

The official told the *Post* that when information passes through “the overseas collection apparatus, the assumption is you’re not a US person.” In reality, however, the “harvesting” of contact lists includes many American citizens as their data passes internationally through the Internet, and is part of the vast illegal NSA spying operations on the population of the United States and the world.

Similarly, the Australian government blandly denies that the ASD’s operations are infringing the rights of Australian citizens. In response to last week’s revelations, a spokeswoman for Attorney General George Brandis told the Fairfax press that all interceptions carried out by Australian agencies were conducted in accordance with Australian law. But the ASD’s data collection undoubtedly intercepts and records information from Australian citizens. Moreover, via the Five Eyes network, Australian intelligence agencies have access to the huge amounts of electronic data stored by the NSA on millions of individuals in Australia and internationally.

Like the previous Labor government, the present Coalition government is continuing the practice using the broad umbrella of “national security” to refuse to answer questions and to block the release of documents. Edward Snowden’s revelations, however, make clear that in Australia as the US, the state apparatus has developed a huge electronic spying operation based on the premise that the population as a whole constitutes a “national security threat.”