Australia: Telstra facilitates US electronic spying

Peter Symonds
15 July 2013

Australian company Telstra signed a secret agreement in November 2001 to ensure that US intelligence and police agencies had unrestricted access to all electronic communications carried in its cables from the Asia Pacific into the US.

The existence of the contract was first exposed by the *Washington Post* on July 6 and subsequently in the *Sydney Morning Herald*. It is one of 28 national security agreements, involving foreign telecommunications corporations with connections to the US, that have been published in full on the Public Intelligence website. The American signatories vary from contract to contract, but include the US Defence Department, Justice Department, Homeland Security and the FBI.

This latest exposure comes on top of revelations by whistleblower Edward Snowden that the US National Security Agency (NSA) has access, via its PRISM program, to the data of nine major Internet companies, including Google, Apple, Microsoft, Facebook and Yahoo. This system of police state surveillance has ridden roughshod over the US constitution and international law.

The Telstra agreement has provided an alternative means for US spying on American and foreign citizens, by allowing access to the vast amounts of Internet and phone data passing through the backbone of international telecommunications—undersea fibre optic cables.

The binding contract with the US Justice Department and the FBI involved a joint venture company, Reach, between Telstra and its Hong Kong partner, Pacific Century CyberWorks (PCCW). The joint venture has since become the largest carrier of intercontinental telecommunications in Asia. It operates 82,300 kilometres of undersea cables in the Pacific linking China, Japan, Australia, New Zealand and Fiji to Hawaii and the continental US. It also has a major cable joining the US east coast to Europe via Cornwall in the US and Brittany in France.

The network security agreement required the company to establish "a facility... physically located in the United States, from which electronic surveillance can be conducted pursuant to lawful US process."

This facility had to be staffed by US citizens "eligible for appropriate US security clearances", who "shall be available 24 hours per day, seven days per week, and shall be responsible for accepting service and maintaining the security of classified information."

Reach and Telstra were required to have the ability to provide:

* Any stored data involving anyone—including Australian and other non-US citizens—making any form of communication with a point of contact in the US.

* Any stored meta-data or information about, rather than the content of, Internet and telecommunications activity.

* Subscriber information and the billing records for any US-domiciled customers, or customers who make a "domestic communication." The latter is broadly interpreted to extend to any electronic communications which "originate or terminate" in the US.

The company had to "take all reasonable measures" to prevent the use of its infrastructure being used for surveillance by a foreign government.

The contract also stipulated that Reach, Telstra and PCCW agreed that non-fulfilment of its obligations would result in "irreparable injury" to the US and "that monetary relief would not be an adequate remedy."

At the time, Telstra was majority-owned by the Australian government. The agreement was undoubtedly vetted and approved by the Howard

government and intelligence agencies, who work in the closest collaboration with their counterparts in the US, Britain, Canada and New Zealand, as part of the "Five Eyes" alliance.

The agreement undoubtedly remains in place, though possibly in revised form after Telstra and PCCW restructured their partnership in 2011, giving Telstra control of the majority of Reach's undersea cables. Telstra has made no comment, other than to acknowledge that the contract was required to "comply with US domestic law."

In fact, as part of the agreement, Telstra facilitates the electronic surveillance by US intelligence and police agencies of Australian citizens and anyone else in Asia and Europe who uses its telecommunications cables with the US.

The *Washington Post* article makes clear that the NSA and other intelligence agencies have used "network security agreements" with Telstra and other foreign corporations to plug into the major international fibre optic cables that carry the vast bulk of telecommunications.

In the past, the US was able to tap into undersea copper cables using listening devices, but that is not technically possible with fibre optic cables. Instead, US intelligence agencies have effectively established secure listening posts at the cable landing stations in the US. As described by the *Washington Post*, foreign corporations are required to establish an "internal corporate cell of American citizens with government clearances" to allow access to the huge amounts of information flowing into the US.

The article explained: "The full extent of the National Security Agency's access to fibre-optic cables remains classified." But documents provided to the *Washington Post* and the *Guardian* by Edward Snowden include an NSA slide entitled "two types of collection", which shows both the PRISM program, involving American internet companies, and a separate program "Upstream."

The *Washington Post* explained: "A diagram superimposed on a crude map of undersea cable networks describes Upstream as collecting 'communications on fibre cables and infrastructure as data flows past.' The slide has yellow arrows pointing to both Upstream and PRISM and says, 'you should use both.'"

This latest revelation is another element of the vast illegal NSA electronic spying operation that gathers and stores information on the phone calls, emails, text messages and Internet usage of the population of the US and the world. The Telstra agreement has exposed the extent to which the Australian government, and major corporations, are deeply involved in these police state measures.