Hot on the heels of data analyst whistleblower Edward Snowden's revelations about the existence of the PRISM electronic surveillance program operated by the United States’ National Security Agency since 2007, we’ve heard some more about communications surveillance – this time with an Australian connection.

The latest story – first reported on Friday by Crikey – suggests Telstra, via a jointly-owned subsidiary called Reach, signed up to an agreement in November 2001 with the FBI and US Department of Justice to participate in surveillance of communications via optic fibre links into and out of the USA.

The company provided physical facilities for interception, kept billing data and maintained the capabilities to collect other data should it be requested.

What’s particularly interesting about the latest revelations is that the US imposed obligations on a non-US company, in this case Reach, to conform to US lawful interception (LI) law.

**Lawful interception**

In most jurisdictions around the world, any organisation or company that operates a publicly-available communications service (a communications service provider or CSP) is obliged to carry out phone taps or wiretaps should they be instructed by law enforcement agencies to do so.

Doha Sam

But how LI is carried out and policed around the world varies greatly. In countries with a strong tradition of the rule of law, carrying out intercepts is separated from the law enforcement agencies who request and use it. Usually, the CSP providing the communications service will carry out the intercept at the request of the agency.

Doing interception this way results in an auditable separation between requesting an intercept and carrying it out, which reduces the risk of illegal interception and consequent corruption.

But in countries for which the rule of law is not as well entrenched, interception is both authorised and carried out by the law enforcement agency. But regardless as to how it is done, there are very few countries that do not have LI capabilities.

The Telstra revelations provide us with some insight into how the US carries out interception of modern communications services.

**Show me the data**

Until the 1990s, communications technologies were comparatively simple to intercept. Communications were circuit switched, meaning an electrical circuit (or an emulation of a circuit) was set up from one fixed end-point (i.e. a phone) to another.

To carry out an intercept all that was required was that at some point on this circuit an electrical tap (or emulation of an electrical tap) be inserted. But in the 1990s things started to change.

The first big change was the move from wireless communications to optic fibre. For decades, long distance communications relied on either satellite or microwave communications links at some point in the communications path. Even if a physical tap on the communications circuit was not possible, communications
could often be intercepted via wireless receivers.

There’s nothing new in communications surveillance. marsmet472

In the 1990s, telecommunications companies began replacing both microwave and satellite links with optic fibre which, compared to wireless communications, is more difficult to intercept.

The second big change was the advent of the internet. Internet communication is based on packet switching – with “packet” in this case referring to separate, segmented lengths of data, sent individually and reassembled in the proper sequence later to make up the message.

The packets are prefixed with a header that contains information as to how the packet should make its way to its destination.

This provides tremendous flexibility, enabling the internet to carry all manner of communications, but it also creates a number of difficulties for interception, the main one being that the internet makes possible the separation of service and location.

In the old fixed-line telephone service, the voice call originates or terminates at the domestic handset, meaning a wiretap at the local exchange will collect communications to or from a given handset.

But with services such as web-based email that's no longer true: a gmail or hotmail account can be accessed anywhere, making the location of an intercept a difficult issue.

Solutions

The latest revelations tell us more about how the US intelligence and law enforcement agencies dealt with these technical problems.

By the late 1990s, people working in the field of communications interception understood the extent of the problems outlined above; and even before September 11, 2001 they had the political support needed to carry out the solution, which was based on a number of obligations imposed on communications companies before they would be given a license to operate.

Importantly, these obligations were imposed not just on domestic operators, but any operator, such as Reach, that provided optic-fibre communications into or out of the US.

warrenski

The most interesting obligation was that the operator must provide a “point of contact within the United States [for] Electronic Surveillance”. These points of contact appear to be “choke-points”; physical installations on US soil through which all communications must pass and so where any communication can be intercepted.

Regardless of where the communication originates or terminates, it will go through one of these choke-points. Of course, extracting a single communication from the mass that passes through these points is another huge challenge, but at least the data can be captured.

The points of contact solve the “location of an intercept” and packet switching problems identified above: the intelligence agencies see all optic fibre communication and all communications pass through one of the “points of contact”.

As well as the “points of contact” there are a number of other requirements on communications service providers. Billing data is often a useful source of intelligence information that may provide information about who has been communicating with whom, and companies must retain two years of billing data. Other data such as internet protocol (IP) and email addresses also has to be retained if requested.

So, what can we conclude from the latest developments? There are no real surprises. We know that lawful interception has been a highly valued (if at times shockingly misused) tool of law enforcement and intelligence
agencies for decades.

Perhaps the most important conclusion we can draw is that the law enforcement and intelligence agencies will not surrender such access easily.

**Further reading:**

See our coverage of the US [National Security Agency leaks](https://example.com).