

## Major Australian telco 'vacuums' all data

by Philip Dorling via digby - The Age - Melbourne *Thursday, Dec 5 2013, 11:27am*

international / prose / post

Australia's leading telecommunications company, Telstra, has installed highly advanced surveillance systems to "vacuum" the telephone calls, texts, social media messages and internet metadata of millions of Australians so that information can be filtered and given to intelligence and law enforcement agencies.



The Australian government's electronic espionage agency, the Australian Signals Directorate, is using the same technology to harvest data flows carried by undersea fibre-optic cables in and out of Australia.

Confidential documents obtained by Fairfax Media reveal the secret technology used to trawl Australians' telecommunications and internet data for analysis by ASIO, the ASD and law enforcement agencies.

All Australian telecommunications and internet service providers by law must maintain interception and data-collection capabilities for government.

The leaked documents reveal that a little-known Melbourne-based company is a key provider of the secret monitoring technology.

Newgen Systems, owned and managed by local telecommunications engineer Robert Perin, is the sole Australian supplier for Gigamon, a large Silicon Valley-based information technology firm that specialises in what it terms "network traffic visibility solutions".

Gigamon's hardware enables telecommunications and IT network administrators to track, inspect and analyse all data flows undetected without affecting the performance of networks.

A key application of the technology is interception of telecommunications and internet data.

In the words of a former Newgen employee, "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."

Confidential Newgen documents describe the Gigamon technology as "a vacuum cleaner" that "sucks up unsynchronised and disaggregated data, filters and sorts it to re-create the original puzzle".

Established in mid-2006, Newgen - now based in Hawthorn - targeted major telecommunications companies and internet service providers, as well as the ASD and ASIO, as potential customers.

Telstra quickly emerged as Newgen's main customer with the first sales of Gigamon hardware occurring in early 2007. Although Telstra has bought a variety of Gigamon systems, a key purpose is "lawful interception" to provide data to ASIO, the Australian Federal Police and state law enforcement agencies.

In April 2010, Newgen submitted a proposal to Telstra's "special projects" group for the installation of Gigamon hardware at 24 metropolitan locations around Australia to meet "a government-mandated regulatory requirement" for interception coverage as Telstra upgraded its network.

An initial rollout of Gigamon systems for Telstra's top 10 exchanges was costed at \$2.7 million, and Telstra's purchases from Newgen in 2010 were worth more than \$3.5 million.

Newgen's first sales to the Defence Department were in 2008 and now total more than \$3 million. Gigamon hardware has been acquired by the Defence Intelligence and Security Group, which includes the top-secret ASD, and by the Defence Materiel Organisation's electronic warfare branch.

The Defence Department's purchases include GigaVUE "traffic visibility nodes" - the standard building block for network monitoring - as well as GigaSMART technology, which modifies captured data, for example by screening out certain types of identity, financial or medical information.

The leaked Newgen documents show that the company provided briefings on new Gigamon hardware to ASD personnel in March 2011, after which Defence purchases increased significantly.

Mr Perin told Fairfax Media that Defence officials "asked a lot of questions [about Gigamon technology] but wouldn't say how or where they are applying it".

Newgen's efforts to win business from Defence intelligence were supported by a partnership with New Zealand company Endace, a leading provider of advanced fibre-optic probes and network recording technology. The Defence Department began buying Endace products in 2008.

Newgen's consultations with the ASD canvassed combining Gigamon and Endace systems with analytical software from Californian software company Splunk in a "technology stack" to produce "real time ... intelligence".

Splunk software is used by the US National Security Agency and Britain's Government Communications Headquarters and enables organisations to analyse "massive streams of machine data generated by websites, applications, servers, networks, mobile and other devices".

Australian Defence intelligence has been buying Splunk software since at least 2009.

A Telstra spokesperson said the company was "required to provide reasonable assistance to law enforcement and national security agencies in response to lawful requests from these agencies ... we only disclose information to these agencies when we are legally required or authorised to do so."

© 2013 Fairfax Media

*[I am not aware of any Aussie that voted for a Big Brother, Orwellian surveillance state; these implementations are unrepresentative and unwanted -- we can put things right by boycotting all*

*major (owned) political parties.]*

<http://tinyurl.com/kq552py>

---

Jungle Drum Prose/Poetry. <http://jungledrum.lingama.net/news/story-896.html>