

“Police State Down Under”, Mass Surveillance in New Zealand: Tapping the South Cross Sea Cable

By [Dr. Binoy Kampmark](#)

Global Research, September 16, 2014

Region: [Oceania](#)

Theme: [Police State & Civil Rights](#)

The Southern Cross undersea cable network is extensive, linking Australia, New Zealand, Fiji and Hawaii to the skeletal framework of the west coast of the United States. In the ownership stakes, Telecom New Zealand has an even half, with Australia's second largest telecommunications provider SingTel Optus coming in at 40 percent. Verizon Business has the rest.

Some weeks ago, rabble rousing cyber activist Kim Dotcom and Glenn Greenwald of *The Intercept* were promising a harvest of revelations on New Zealand's role in the surveillance fruit salad.^[1] The Government Communications Security Bureau (GCSB), which sounds like a benign desk shuffling company, is the country's willing accomplice in the Five Eyes arrangement. Between 2012 and 2013, a metadata surveillance system was created, centred on the Southern Cross cable network. Big eyes indeed.

Seeing that the unimaginative were in charge of the operation, or at the very least naming it, the surveillance program obtained the code name “Speargun”, involving the covert installation of tapping equipment on the cable link. As to be expected, the entire operation took place in stages – the first being the initially seedy point of tapping the cable; and phase two being the use of “metada probes”, the first being ready by mid-2013.

As should be familiar by now, such probes are fundamental to obtaining the data from communications encompassing time, dates, senders, email addresses and phone calls, not to mention the substantive content.

The New Zealand prime minister, John Key, condescended to explain that internet surveillance laws enacted in 2013 were done so for a very simple reason: to amend “an ambiguous legal framework”. The GCSB legislation had triggered a chorus of “alarmist” calls, but, he said not too reassuringly in parliament, NZ citizens had nothing to concern themselves about.

His third reading speech delivered in August last year says nothing about what is actually to be done, but what has always been done in the spooks business. The work might reek of intrusive molestation, but all to the good. What the PM simply reiterates are those swill bucket observations that are second nature in the advertising business – the need to “protect New Zealanders” from “threats” that are “real and ever-present”.^[2]

Key has never even felt a need to explain what these threats might be, ignoring the greatest rule of intelligence gathering in a democratic state: Gaps are necessary. Apertures in the system tend to be their salvation, the cautionary protection for good governance. But he doesn't want to give that side of the bargain up. Just back obstinate paternalism, and hope

for the best. Hence, it was sufficient for him to say that he had “been briefed by intelligence agencies on many issues, some of which have deeply concerned me.”

As paternalism is the greatest incentive to mendacity (parents tend to deceive their children in the name of protecting them), Key has been found wanting, claiming that there has been no instance of mass surveillance in New Zealand. Greenwald had touched a nerve in appearing with Dotcom ahead of the country’s election on September 20. “Mr Dotcom’s little henchman will be proved to be incorrect because he is incorrect.... There never has been mass surveillance and there is no mass surveillance.”^[3] But there was Snowden, ever ready with a bucket of numbingly cold water. “The Prime Minister’s claim to the public, that ‘there is no and there never has been any mass surveillance’, is false.”^[4]

The egg on Key’s face seemed to be accumulating, with Snowden explaining that, in the course of his work, he “routinely came across the communications of New Zealanders” connected with “a mass surveillance tool we shared with GCSB, called XKEYSCORE.” The particular access is “granular” in nature, having little to do with cybersecurity purposes but “used primarily for reading individuals’ private email, text messages, and internet traffic.”

NZ intelligence personnel are not merely involved in the use of XKEYSCORE but also active development of “mass surveillance algorithms for it.” Suggestions from the Key camp are that such a mass accumulating program might have been flirted with, but never actually embraced. Snowden roundly dismisses it.

The former NSA contractor adds a bit more material here to his previous disclosures. Analysts, for instance, can make use of a “checkbox” which conceals “the results of mass surveillance in New Zealand”. In intelligence speak, this is the “Five Eyes Defeat” filter. The very presence of such a function howls for recognition that Key and company have been rather slap dash with the verite.

Correcting legal frameworks at this end of the business is much like covering the bases of a criminal with the tracks still warm. That, by definition, is how most intelligence networks function – an extra-legal realm of operation that shirks and hides from the legal net in order to combat illegality. To allow a state to pursue such conduct does not merely advocate abuse, but the highest logic of inefficiency.

Time for Key, perhaps, to embrace an election slogan aligned with comments from the GCSB. In the words of a spokesperson, “We don’t comment on matters that may or may not be operational.”

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

Notes

^[1]

<https://firstlook.org/theintercept/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/>

^[2] <http://www.stuff.co.nz/national/politics/9070452/GCSB-Prime-Minister-John-Keys-speech>

^[3]

<http://tvnz.co.nz/vote-2014-news/key-dismisses-dotcom-s-henchman-over-spy-claim-607965>
2

[4] <https://firstlook.org/theintercept/2014/09/15/snowden-new-zealand-surveillance/>

The original source of this article is Global Research
Copyright © [Dr. Binoy Kampmark](#), Global Research, 2014

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Dr. Binoy
Kampmark](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca