Is GCSB spying on tens of thousands of Kiwis?

Keypoints

This week's revelations about spying on tens of millions of US citizens by the US equivalent of the GCSB raises questions as to whether GCSB is also extensively spying, or might in the future. This is also another case study for the power of Big Data following our case study, *Big Data in business – father learns of teenage daughter's pregnancy from retail chain*.[1]

This article first appeared in National Business Review online on 9 June.

June 2013

Today, the GCSB is front page news. But it's Peter Dunne's picture on the front page, when the bigger story remains on the back pages, hardly debated over the last few weeks.

It's not like that in the US, as President Obama is finding. On Thursday, the US equivalent of the GCSB – the National Security Agency (NSA) –was rumbled, in scoops by the Washington Post and the Guardian. The scoop was a copy of a **secret court order**[2] requiring Telco, Verizon, to provide metadata – if requested by NSA - on phone calls by all business and Government customers. The general view is that there are such orders as to their other customers, and the other Telcos have to do the same too. Press reports say NSA is collecting metadata on tens of millions of US citizens.

That's not all that's been leaked in relation to the NSA over the last two days. Now confirmed is that NSA also uses a program called PRISM to access extensive user content held by Google, Facebook, Microsoft, and Apple: although targeted at non-US citizens, plenty of content for US citizens is collected too. That data collection programme is explained in slides revealed by the Washington Post.[3] Expect the NSA to hold Kiwi's user content for example, as it flows through the States.

President Obama is under strong attack from both the left and the libertarian right. Americans are generally quick to understand the need for surveillance, but many also recognise the need for controls and boundaries.

Dealing with the metadata relating to phone calls –PRISM may relate to issues for GCSB too - the metadata obtained by the NSA includes details of the phone called from, the phone called to, duration of the call and the "*unique identifiers*" of those phones (essentially, the equivalent of phone numbers and the underlying identifiers used by Telcos). It excludes what was said in the call.

Use of such metadata was a key focus of the Kitteridge report into the GCSB, and a key focus of the GCSB Director's unsatisfactory and contradictory press release, on which I wrote last Saturday, *GCSB director's report alarming*.[4]

The GCSB are likely to be using the metadata in the same way: to track groupings suspected of terrorism and other crime, by tracking what phones are used to call other phones. The calling patterns say much. If they give rise to enough concern, the GCSB can then take the next step of listening to the calls after following the process in the GCSB Act.

Is GCSB spying on tens of thousands of Kiwis?

I've referred to "*phones*" rather than the people calling and receiving, because the NSA and the GCSB don't directly track the identity of the people. They can't do that directly. On a landline in a flat shared by several, who called?

It's what the GCSB Director doesn't say that is telling. He says, "*An example of metadata is the information on a telephone bill such as the time and duration of a phone call, but not the content of the conversation or identification of the people using the phone.*"

It's the identification of the phone – the unique identifier - that the GCSB gets, not who used the phone. But of course, having the phone's unique identifier is usually the same as knowing who the caller is, and the calls of interest are to other people of interest. That combination nearly always identifies the caller, and the GCSB can use other information to stitch together the pieces. In other words, contrary to what seems to be implied by the Director, collecting phone unique identifiers is close to identical to collecting "identification of the people using the phone." We have little choice but to trust the Director to get these things right. Spun press releases don't help that.

Forbes today has a good article, *How The NSA Tracks Your Calls*,[5] about how the NSA uses the metadata. It's all part of the Big Data explosion in business and government, by which datasets can be matched and tracked using vast computer power and analytics, as we explained in our article, *Big Data in business – father learns of teenage daughter's pregnancy from retail chain*.[6] The metadata from phone calls can be matched with other massive datasets. Forbes suggests that the NSA may stockpile this metadata (comprising billions of pieces of information) for use when and if needed.

The NSA can derive considerable information from such data, even though they aren't listening to the calls. Much information can be reverse engineered to de-anonymise data, across multiple data sets, a concern increasingly being noted by privacy and security experts.

It is likely that GCSB has been tracking suspected groups by way of tracking who is calling whom and their calling patterns. Is this confined to limited people who are under focus, as the press release implies, as that release refers to review of only 88 people? How can we be sure as to surveillance of Kiwis, given for example the footloose way GCSB has proceeded in strained interpretations of clear-cut legislation, the Dotcom fiasco with simple errors made, and the Director's contradictory press release? Just as the Director has used words smoothly by noting that metadata does not include "*identification of the people using the phone*" when that in net terms is what in fact is happening, has there been a way to avoid reference to wider collection of data, similar to what is happening in the US? If the Keystone Cops way the Police handled the FBI request is any indicator, has the GCSB taken an approach facilitative of US wide requests?

And even if only up to the 88 people have had their metadata tracked, that refers only to surveillance as to Kiwis, which the Act does not permit. What of international phone calls between people in New Zealand and people overseas, which is more within the focus of the Act, and further outside the restriction on domestic surveillance? What about internet communications? Is the GCSB collecting much or even all of that metadata, and that's outside what is covered in the Kitteridge report? The US and other surveillance agencies would benefit from extending their Big Data footprint in this way, so the GCSB might be encouraged to feed that data into their datasets.

Why care about this? It is a small step to abuse of spying powers, negatively affecting New Zealanders, in an area that is difficult to effectively control and monitor. Even our tame country can have Kafka-like scenarios: As that highly reliable lawyer's resource – Wikipedia – summarises, Kafka's book, the Trial, "*tells the story of a man arrested and prosecuted by a remote, inaccessible authority, with the nature of his crime revealed to neither him nor the reader.*"

Is GCSB spying on tens of thousands of Kiwis?

Say GCSB doesn't do this widespread surveillance now: what about the future?

As I pointed out last week, we must have robust ability to allow covert surveillance. GCSB have an important role. My own view is that there should be the ability to track metadata within confines. The key is balance, control and monitoring. As Forbes said yesterday:

> *Balancing national security against the protection of civil liberties is obviously a difficult challenge. And it's a conversation we as a nation must continue having. It is important to realize, however, that the technology used to identify threats and keep us safe are maturing and developing rapidly. Technology is not a cure-all to the security v. civil liberties challenge, but as the tools become more sophisticated it becomes easier to zero-in on the bad actors without compromising the privacy of the rest of us.*

Finally, I repeat the health warning in my last article: we don't know whether there are things under the bonnet that justify the approach taken, but that seems unlikely. There are things GCSB can do to reassure New Zealanders – the need for confidentiality does not stymie that - but they haven't taken those steps.

---

1. http://www.wigleylaw.com/assets/Uploads/Big-Data-in-business.pdf

2. http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order

3. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1

4. http://www.nbr.co.nz/article/gcsb-directors-report-alarming-ck-140623

5. http://www.forbes.com/sites/siliconangle/2013/06/07/how-the-nsa-tracks-your-calls/

6. http://www.wigleylaw.com/assets/Uploads/Big-Data-in-business.pdf

Wigley+Company
PO Box 10842
Level7/107 Customhouse Quay, Wellington
T +64(4) 472 3023 E info@wigleylaw.com
and in Auckland
T +64(9) 307 5957