Proposed GCSB powers to control Telcos' network choices

Speedread

GCSB and its Minister will have wide powers to control network component and configuration choices under the Telecommunications (Interception Capability and Security) Bill (TICSA). Governments need powers to deal with cyber-crime and cyber-terrorism, and it is not realistic to have all those powers the subject of close judicial input (which is one of the key planks in controlling the powers of the executive: the powers of Ministers and officials). But clearly there must be sufficiently strong controls on the exercise of the executive's and GCSB powers; the recently uncovered abuses of those powers by GCSB illustrates that the status quo is not adequate. Telcos should not be unreasonably forced to spend more money and configure networks differently, unless justified.

In this article we outline where the Bill currently draws the balance, as a background to the question of where the line should ultimately be drawn. A balance between the views of civil libertarians and hawks. Government has noted it is open to appropriate change. We don't express views on what is right and wrong.

May 2013

Two related Bills have just been released: the GCSB Bill, to amend the existing GCSB legislation, and TICSA. TICSA:

- amends the telco network interception regime first introduced around 9 years ago; and
- brings in, for the first time, GCSB and Ministerial powers to require network components and configuration to reduce what is called "*significant network security risk*".

This piece deals with those new powers.

The regime only applies to network changes and not the status quo network, save that network operators must also notify the GCSB when they become aware of existing network security risks (including risks as to inter-connected foreign networks).

Obligations apply where a "*network operator*" – which is defined widely – plans changes in key parts of the network, such as the network operations centre, data aggregation (stored or transitory), customer information databases, etc (plus other things added to the list by regulation supported by the GCSB Minister, usually the PM, within the framework in TISCA). Applicable changes include changes to equipment, systems, services, control and ownership (ie, this is wide and granular). Early on in its plans (e.g. before going to RFP), the network operator must tell GCSB of its plans, unless GCSB has carved out a requirement to disclose by a prior notice.

There's a process by which GCSB and the operator agree the change is acceptable. If there isn't agreement, then, ultimately, the GCSB Minister makes the decision as to what the network operator can and can't do. There's a framework for decision making, revolving around the Minister being satisfied that the powers are exercised to "*prevent, mitigate or remove a significant network security risk*". One issue is how that overall framework should be structured.

Proposed GCSB powers to control Telcos' network choices

A "*significant network security risk*" is defined as a "*significant risk to New Zealand's national security or economic well-being*". In theory there can be judicial review of the Ministerial decision. In practice, judicial review is a blunt instrument for controlling executive powers. The general success rate on judicial review applications, for example, is not high. Further, while the network operator has the right to submit on why its network choices are appropriate, the classified nature of the decision making will often mean that the operator does not know what to say and what is relevant. There's a "*punching at clouds*" element to this. The operator can be forced to take inefficient and costly network implementations (despite some theoretical protection in TISCA). If there are to be controls, checks and balances, other mechanisms may be needed (such as adequate monitoring by independent inspectors).

It's challenging to set the framework so that it is workable while containing adequate protections. Take the definition of "*significant network security risk*". That includes, as a separate item from "*risk to security*", risk to "*economic well-being*". On its face, that all seems understandable. But, play out the debate in the US against Huawei. Some critics of what the Senate Committee did believe that the attack on Huawei boils down to trade protection: keep the Chinese out to shore up domestic US suppliers, under the guise of cyber-risk. Now that seems to be "*risk…to economic well-being*", highlighted in NZ by the GCSB Minister's obligation to consult the Minister of Trade before making decisions on the network, in a situation where external control and monitoring of executive decisions is challenging. As noted above, there's the "punching at clouds" aspect to all this, in the context of complex multi-faceted decision-making, even though it can be argued that the overall framework restricts the Minister's discretion.

This highlights how hard it is to get legislation like this correctly balanced to ensure the ability to deal with cyber-terrorism and the like, while sufficiently protecting Telco rights.

Some are saying that the legislation simply formalises what informally happens already between Telcos and GCSB. That will not do as a justification. There is a world of difference between voluntary compliance by telcos and forced compliance using executive powers.

The recent Dotcom GCSB fiasco, with revelations of over 80 other breaches of the GCSB Act in relation to New Zealanders, shows how important it is to get this right. If the simple stuff is handled badly, what about other things? And those 80+ errors appear to be GCSB Act 101. The Rebecca Kitteridge report on GCSB is valuable reading in this area, including for highlighting how important the work of GCSB is, where, because of its covert nature, only the bad stuff tends to emerge. Those on both sides of the debate (civil libertarians and hawks) should look to it for the balance. It is simply not enough to fly the civil liberties flag alone nor to allow substantial discretion.

Having said that about the Kitteridge report, it may be that GCSB officials get off lightly in that report as to their apparent breaches. The section in the GCSB Act on not spying on NZ'ers is easy to read and simple. It is in a short Act of only 17 pages, an Act that primarily governs what the GCSB officials can do. Also, the computer crimes and personal privacy interception

Proposed GCSB powers to control Telcos' network choices

provisions in the Crimes Act must surely be understood by these specialists in pursuing cyber terrorisim, hacking etc (after all, those Crimes Act provisions are core to the subject matter of their day jobs: it's also a key part of how the scope of their roles is defined as well). The potential offences apply to GCSB people, outside the legislative carve-out in the GCSB Act (and any relevant carve out in the Crimes Act). If someone at GCSB does not come within a carve out, they can commit an offence under the Crimes Act.

Yet the ability to spy on NZ'ers, says the report, was even embedded in the GCSB operational guidelines. The two stated justifications used by GCSB seem tenuous. Doing activities as to New Zealanders on request from SIS (which can investigate as to locals) as an agent of SIS (under the warrants SIS obtained) is a long bow. Apparent reliance on the purpose and objective provisions in the Act is said to justify that. That is tenuous enough, on its own, given the focus there on foreign intelligence. But the section before the section disallowing activities as to locals makes a point clearly and simply. Interception of communications is allowed "*only if the purpose of the interception is to obtain foreign intelligence*." The agency idea is a stretch.

And the second ground is said to be that metadata (such as the sort of information in a telephone bill) is not covered as it is not "*communication*". If it is assumed that GCSB was right in this, and yet got the information by interception in a manner otherwise covered by the computer crimes and/or personal privacy regime in the Crimes Act, then the GCSB Act carve-out does not apply, and there may be an offence (if there's no Crimes Act carve out). That might include where there was inappropriate use of interception permitted by warrant, if that happened. But, anyway, given the way "*communication*" is defined, such metadata appears to be included (again, this is an easy-to-follow part of the Act). As to how metadata is handled on the agency basis above falls to be considered in the way noted above.

Of course we don't know the full facts in this understandably covert area and there may be wider justification. Perhaps that will emerge when decisions are made as to whether or not to exercise discretion to prosecute under the computer crimes regime in the Crimes Act, involving considerations around gamekeepers being held at least to standards applied to poachers, etc. Ms Kitteridge emphasises the bona fides and best intentions of the officials involved – and that is an appropriate factor in exercising discretion -and some officials might legitimately say that the manual permitted it and they can rely on that (plus there may be factual issues around whether carve-outs apply to particular officials).

Public servants doing, for us, a difficult job in difficult circumstances.

We shouldn't be taken as encouraging prosecution, nor saying there are breaches, as we don't have all the information.

But at the least, this real life situation highlights that it is important to get the balance right in this new legislation. Even the simple stuff can be handled poorly.

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
www.wigleylaw.com