

Submissions to the Select Committee on the New Zealand Intelligence and Security Bill 2016. What should we be concerned about?

1. The powers of the spy agencies – the Government Communications Security Bureau [GCSB] and the Security Intelligence Service [SIS] are enormously expanded from their powers in 2012.

2. Central to this expansion is the fact that GCSB spying on New Zealanders, completely forbidden before 2013, is now part of GCSB functions by legislation.

3. The Director-General of Intelligence and Security may retain and disclose to public authorities, domestically or overseas, any "incidentally-obtained intelligence", which is a loophole for mass surveillance.

4. Incidentally obtained data may be shared with other agencies in New Zealand as well as those overseas, where the overseeing Minister so chooses.

5. (a) While a more stringent warrant system is set out in the new legislation, there are potentially dangerous gaps in the law. The Bill does not require warrants to carry out "lawful activities" but these are not clearly defined. Is following a suspect 'lawful'? Is entering a house where a crime is suspected of taking place 'lawful'?

(b) The Bill proposes new types of warrants, targeted warrants and purpose-based warrants that are intended to enable the agencies to obtain approval to intercept communications for class interceptions. This means large groups of citizens can be targeted, especially if they can be connected to overseas activity.

The justification for the legislation is that it would enable the SIS to obtain approval to intercept communications for such purposes as identifying whether New Zealanders are fighting with ISIS in Syria, whether or not the agency knows their names. But under the new legislation the agencies can intercept the communications of one or more persons or classes of persons or of "places" (for example, the location of an ISP), or all or any communications sent from or to a nominated overseas country. Note that this would net an incredibly large number of people who have contact with a 'suspect'.

(c) Finally, as of 2013, urgent warrants can be sought in special cases, including where someone's life is at stake or there is a serious threat to New Zealand's national security. This means the agencies can take action as long as they get a warrant within 24 hours. In the one case of this usage that has come to light, not arrest or prosecution followed, suggesting that the procedure was not properly used.

(d) The checks and balances in the proposed system are almost all 'in house' with sign-off being envisaged by the Attorney-General and the Commissioner of Security Warrants and the only independent oversight role for compliance is the Inspector-

General of Intelligence and Security. There is still no direct and/or adequate parliamentary oversight.

[Additional note: The draft Bill sets out a new system of warrants, data sharing and oversight. A number of commentators have declared the Bill's requirements for the issue of warrants for surveillance as relatively robust. But for those distrustful of the agencies, on the basis of their given history and/or the demands of their Five Eyes brethren, there are potential problems. "Trust us, we know what we're doing' would be a more credible message if those running this system had a track record to justify the public's faith in them. The 'jihadi brides' fiasco was one recent example of scaremongering by the SIS, and the Government". [Gordon Campbell, *Scoop*] The Dotcom case, the Zaoui case and the recently revealed Tony Fullman case give no grounds for reassurance.

6. The Government clearly intends to discourage whistleblowers. A new offence will be created for people who hold a Government security clearance, or those given access to classified information, who wrongfully communicate, retain or copy 'classified information'.

The proposed new section 78AA of the Crimes Act would impose a five-year jail term for passing on, retaining, or refusing to return "classified information". And it would apply this penalty not just to Government agents who hold that classified information in the course of their jobs - but to anyone who has ever held a security clearance, and over all classified information whether or not they've ever seen it before.

A large number of public servants hold security clearances in the course of their work. MPs and Ministers automatically hold such clearances. Various people in the IT sector can be required by the GCSB to obtain a security clearance in order to keep their jobs. One reading of this is that any of these people could be jailed for making a copy of, or forwarding, any articles, even by main stream media, which are based on leaked information.

7. Intelligence agency employees who encounter evidence of wrong-doing can make a protected disclosure to the Inspector-General of Intelligence and Security. But if they give information to others or the media they face a prison sentence of up to five years in jail. This presents a dire threat to anyone considering going public about activities.

[Additional note: In Australia, a whistleblower in a spy agency complained to the IG and nothing happened because, mysteriously, all the documents related to the case could not be found!]

8. The Privacy Commissioner can investigate breaches by the intelligence agencies but can only make recommendations to agencies and to the Prime Minister, which the latter is not obliged to follow.

9. SIS and GCSB operatives will be able to acquire, use and maintain "any identity information necessary to maintain the covert nature of their work and keep

themselves safe” and ensure that anyone else assisting them in these deceptions is similarly exempt from civil or criminal proceedings

[Additional note: This means we trust those involved to only use their disguises within ethical and legal bounds and not for any private purpose]

10. Under the Privacy Act it is perfectly lawful for an agency such as a business holding customer information to disclose it to authorities where reasonable grounds exist for believing it is necessary for law enforcement, detecting offences and so forth. The intelligence agencies have now been added to this list. The Police are likely to produce evidence as to why they need access to information but all that is required of intelligence agencies is their say-so that the information is needed, and the information holder could be easily duped or bullied into providing the information.

[Question: Is pressuring a data holder a ‘lawful’ activity which does not need a warrant? Not even the corporate giants like Microsoft and Google have been able to resist the demands of the intelligence agencies to give out customer data. Even Sir Michael Cullen, who carried out the recent review of the Security Intelligence Service and Government Communications Security Bureau, said New Zealand's spy agencies already have "open slather" access to Kiwis' personal information through Government agencies as well as private companies including banks.]

11. Individuals cannot complain to the specialist tribunal that hears complaints against other agencies and can award damages.

12. Finally, the Bill's definitions of the GCSB's functions incorporate widely drawn terms such as "information assurance and cybersecurity" and "information infrastructure" that cover, for example, things such as metadata and big data. There is a serious risk that the ever-expanding cybersecurity function of the GCSB allows it more access to data. Note above in 3 that the Director-General of Intelligence and Security may retain and disclose to public authorities, domestically or overseas, any "incidentally-obtained intelligence’.

14. The Chief Human Rights Commissioner David Rutherford has said the proposed changes in the Bill were "a significant improvement" with stronger authorisation for spying warrants, greater oversight of the agencies, and strengthened requirements regarding compliance with human rights law, but there were aspects of the Bill which were still a concern. "Chief among these is the definition of national security," he said.

Further Comment

Submissions questioning the existence of the spy agencies, and/or their Five Eyes partners, will be entirely ignored unless they are connected to the specific content of the Bill. Nevertheless, without cognisance of the wider issues, the detail becomes almost meaningless.

- (a) There is plenty of historical and contemporary evidence to support the case that the GCSB should be closed down and its essential functions redistributed to other more transparent organisations. In criticising the new Bill we must not forget that we are putting aside the fundamental point to be addressed, and sidelining critical aspects of surveillance, civil liberties, and political control.
- (b) Concentrating on our spook agencies in isolation and ignoring the incredibly large African/Indian mammal in the room essentially means much of the NZ legislation is irrelevant because of the Five Eyes integration. The big brothers 'take it all, analyse it all' data mission, and the ruthlessness with which this goal is pursued, means any perceived threats to the 'national security' of any of the partners will mean national laws are trampled underfoot and our spook agencies will tow the line whether it involves breaking NZ law or not. To believe that we can legislate in isolation is intentional or ideological madness.

Background: The official version

The [New Zealand Intelligence and Security Bill 2016](#) is the most significant reform of our intelligence agencies in our country's history. It was introduced into Parliament in August 2016.

The key aspects of the Bill are that it:

1. Creates a single Act to cover the agencies and their oversight bodies, replacing the four separate acts that currently exist.
2. Enables more effective cooperation between NZSIS and GCSB, enhancing their effectiveness while still ensuring there is appropriate transparency and accountability around their activities.
3. Strengthens [oversight](#) of the activities of NZSIS and GCSB.
4. Introduces a [single warranting framework](#) for intelligence collection activities and tightens up the authorisation framework for granting warrants.
5. Brings NZSIS and GCSB [further into the core public service](#) increasing accountability and transparency.
6. Clarifies arrangements for the [use of cover and assumed identities and immunities](#).
7. Sets out the role of the [National Assessments Bureau](#) in legislation for the first time."