InternetNZ

Submission to the Independent Reviewers of Intelligence and Security

14 August 2015

InternetNZ

1. Introduction

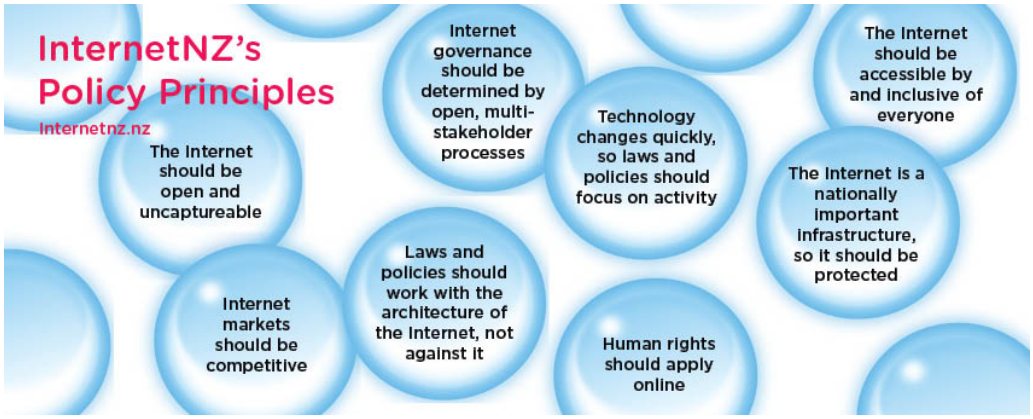
1.1. InternetNZ greatly appreciates the opportunity to provide the Independent Reviewers with our thoughts and views on what legislative and oversight changes are needed, or desirable, for New Zealand's intelligence agencies.

We are committed to an open and uncapturable Internet

1.2. As an organisation that works to promote the Internet's benefits and uses and protect its potential, we care passionately about Internet-based communications and the opportunities that the Internet brings. We work for a better world, through a better Internet.

1.3. This submission focusses on intelligence and security matters as they relate to the Internet, and the institutional frameworks and transparency arrangements that are important to maintain an open and uncapturable Internet. Our comments in this submission reflect our policy principles (set out below).

Figure one: InternetNZ's policy principles



1.4. As a membership-based organisation we will not be attempting to answer the general questions within the consultation document. Instead, this submission is structured to set out our views on:

a) the need to protect human rights online [section 2]
b) ensuring that intelligence agencies do not undermine Internet Security [section 3]
c) the need to improve the Rule of Law in the legislative and oversight frameworks of the intelligence agencies [section 4]
d) greater transparency of intelligence agencies and their interactions with New Zealand organisations [section 5]
e) the need to improve the definition of private communication [section 6].

1.5. We welcome the opportunity to discuss our submission with you. Please contact Ben Creet, Senior Issues Advisor at ben@internetnz.nz or on 021 246 3228 for further information.

Jordan Carter
Chief Executive

InternetNZ

2. Human Rights need to be protected online

2.1. Online and offline, people should be protected by their fundamental human rights, such as the right to privacy, the right to freedom of opinion and expression and the right to seek redress when they are harmed. Nation-States especially have an obligation to see that these rights are protected regardless of whether they are exercised on the Internet or on the street.

2.2. InternetNZ has particular interests that New Zealanders' human rights apply online. The Internet should be accessible by, and inclusive of, everyone. The benefits of the Internet, for social and business use should not be undermined by fear or concern that New Zealanders are being monitored, observed and tracked by intelligence agencies in a way that they would not be monitored offline.

3. Protecting the security of the Internet

3.1. The Internet is nationally important infrastructure and should be protected. We note that the GCSB has a dual role - one as a signals and foreign intelligence agency, and another as a cybersecurity provider and expert. We welcome the GCSB's work to increase its cybersecurity role through the National Cyber Security Centre. We want to see the Internet protected and New Zealanders protected from malicious actors using the Internet.

3.2. However, we remain concerned that, through its foreign and signals intelligence mission, the Bureau could be involved in weakening the cryptography that underpins much of the Internet's security. In 2013 it became clear that the NSA worked to undermine commonly used encryption methods to further its own ability (and its Five Eyes partners' ability) to "sniff it all, know it all".[1]

3.3. Weakening the security of the Internet is bad for everyone, it makes Internet users less secure and it undermines the role and mission of the Bureau to provide cybersecurity protection.

3.4. We recommend that New Zealand's intelligence agencies commit to the public that they will not participate in or support any efforts to undermine security measures or cryptography protocols which businesses or individuals might use to protect themselves.

4. Improving the Rule of Law over intelligence agencies and their work

4.1. We want to make sure that our existing systems of checks and balances should apply to intelligence agencies. Any public service department that has intrusive powers into the lives of New Zealanders (both online and offline) should operate under laws which clearly set out the scope and limits of those powers. Exercise of those powers should be subject to independent oversight, including judicial oversight at least where human rights issues may arise.

4.2. Ministers are either responsible for, or jointly approve, warrants for the NZSIS or GCSB to undertake their lawful intercept, surveillance or search powers. This level of involvement by politicians in the use of intrusive powers by intelligence agencies is undesirable because it creates room for inconsistent, arbitrary and political considerations of the day to enter into decision making about intrusive powers.

[1] See: www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption
www.stuff.co.nz/national/politics/10046942/NSA-tells-NZ-spies-Sniff-it-all

Simply put, the current level of Ministerial involvement in warrants undermines the rule of law in New Zealand. We do not agree, as a matter of principle, with this level of Ministerial involvement in the activities of intelligence agencies on the Internet (we raised this issue in our submission on the *Government Communications Security Bureau and Related Legislation Amendment Bill* in 2013)[2].

4.3. You are in a position to recommend major legislative improvement to strengthen the Rule of Law by removing direct Ministerial involvement in approving warrants and appointments.

4.4. Currently, interception warrants are issued by a Commissioner of Warrants, who is appointed on the recommendation of the Minister. This process fails the test of political independence, risking perceived or actual violation of the rule of law.

4.5. Instead, GCSB and NZSIS warrants should be approved by an appropriately skilled, cleared and available judicial figure or group. For example, if the level of work from approving warrants should necessitate a group of judges, then a Court akin to the USA's Foreign Intelligence Security Court could be contemplated. However, should this level of investment and process not be required due to a lack of work, then we would still suggest that the Commissioner of Warrants should be required to be a current Judge, or small number of Judges, appointed by an appropriately senior judicial figure such as the Chief Justice.

4.6. We note that, while the GCSB is a Public Service Department (appearing on Schedule 1 of the State Services Act 1988), the appointment of its Director is not the same as that of other Chief Executives of public service departments. The appointment process for Chief Executives are well-understood and involve clear, transparent processes for the Governor-General to accept, or not accept, appointment recommendations by the Commissioner.

4.7. It is our position that, in order to enhance the Rule of Law over the intelligence agencies the Reviewers should recommend the following changes.

a) Remove Ministers from the process of approving warrants for intelligence agencies, ceding responsibility for warrants to an appropriate judicial figure or group of Judges. Further, the appointment of the Commissioner of Warrants, or a dedicated court bench, should be made the responsibility of the Chief Justice (or another suitably senior judicial leader).

b) Place the appointment processes for the Chief Executives of the GCSB and the NZSIS within the broader, more transparent process that the State Services Commissioner runs for Chief Executives of public service departments.

c) The Inspector-General of Intelligence should be appointed by a person, or group, independent from the Minister or Cabinet. Possible models include a State Services Commissioner appointment processes, or a Parliamentary appointment process as per the Auditor-General.

5. More transparency is needed

5.1. We believe in an open and uncapturable Internet. We understand the need for secrecy relating to operational details that relate to national security. However, intelligence agencies exist to serve and protect New Zealand and its people. Events in recent years have dented public confidence and trust in New Zealand's intelligence agencies (e.g. Kim Dotcom case, Snowden documents, the investigation into the NZSIS's release of official information to a prominent blogger). As such, the level of

[2] A .pdf copy of our submission can be downloaded here: https://internetnz.nz/sites/default/files/submissions/gcsb_submission_internetnz_final.pdf

public reporting and transparency about the agencies needs to increase. Giving Parliament and New Zealanders a sense of the level of work, and the nature of the work, that the intelligence agencies engage in should be a major consideration for the Reviewers.

5.2. We think that an important aspect of this greater transparency is enabling New Zealand organisations to release regular transparency reports. Internationally, transparency reports have been used by Internet-based companies to let their customers understand how often they are being issued with warrants and orders to produce information about individual customers.

5.3. Allowing New Zealand organisations to release transparency reports about the number of requests they receive, and the number of security or interception warrants they are served, is one way to increase the level of transparency around intelligence agencies.

5.4. In his July 2015 speech to the Institute of Intelligence Professionals, the Privacy Commissioner outlined his office's new project to work with New Zealand organisations to publish template transparency reports about law enforcement requests and warrants.[3]

5.5. Trade Me produces annual transparency reports[4], including the number of requests that it receives from the NZSIS. We applaud this effort, and the work of the Privacy Commissioner to spread transparency reporting, and encourage you recommend changes that would ensure that New Zealand companies continue to have the ability to publish transparency reports.

6. The definition of Private Communication needs to be improved

6.1. You have specifically asked questions seeking people's view on the definition of private communication in the GCSB Act 2003 (reprinted below for ease of reference).

Figure two: definition of private communication (s4, GCSB Act 2003)

private communication—

(a) means a communication between 2 or more parties made under circumstances that may reasonably be taken to indicate that any party to the communication desires it to be confined to the parties to the communication; but

(b) does not include a communication occurring in circumstances in which any party ought reasonably to expect that the communication may be intercepted by some other person not having the express or implied consent of any party to do so

6.2. The concept of a private communication is central to the GCSB Act and whether a warrant is required to intercept the communications of a New Zealander. This definition has been incorporated into a number of other enactments.

6.3. A clearer definition of "private communication" would have a number of benefits:

a) New Zealanders would have a better idea of which communications count as "private" for surveillance and law enforcement purposes
b) Intelligence agencies would have clearer guidance on the exercise of their powers

[3] https://www.privacy.org.nz/news-and-publications/speeches-and-presentations/privacy-commissioners-speech-to-nz-institute-of-intelligence-professionals/ accessed 10 August 2015
[4] http://www.trademe.co.nz/trust-safety/transparency-report-2015-by-trade-me/

c) Clear drafting of legislation under Legislative Advisory Committee guidelines gives certainty and supports the rule of law.

6.4. Other submissions may address the applicability of the definition to in-person communications. In this submission, we address particular problems where the definition is applied to communications over the Internet. We have identified a number of inadequacies, listed below.

The concept of 'party to a communication' is not defined

6.5. It is not clear whether this only relates to the people (or machines) sending and receiving the communication, or whether an ISP, or an application provider are considered party to the communication.

6.6. We think that the parties to a private communication should only be defined as the sender and receiver(s) of the communication content.

Who constitutes 'any party'?

6.7. The definition then refers to 'any party', which presumably is intended to be read as 'any party to the communication'. However, this is not actually stated or defined.

6.8. This could enable someone to opportunistically interpret 'any party' to include some other third party to the communication such as a network, service or application provider.

- Is Chorus, as the network provider for UFB party to a private communication that take place across its fibre network?
- Is Spark party to a Messenger (Facebook's messaging app) communication sent by one of its customers?

6.9. This lack of clarity undermines the definition of private communication and should be addressed through clear, simple drafting.

'Reasonably ought' is a difficult legal test to unpick

6.10. If this 'any party' reasonably ought to expect that the communication may be intercepted, then the communication is not considered private. A reasonable person test, combined with the word 'ought' creates a rather complex legal definition where an existing legal test (a reasonable person) is combined with the idea of that person 'ought' to expect something to occur. If something were to occur 25% of the time, would that mean a person ought to reasonably expect it to occur? Or is the definition intended to rely on a balance of probabilities?

The use of 'may' is inconsistent with good drafting

6.11. The use of the term 'may' in (b) is problematic because it is unclear how the reader of the definition should interpret whether someone 'may intercept' a private communication. 'May' should be used in law in relation to the discretionary use of a power, or permission, rather than to describe a possibility or probability of something occurring.[5] Using may, and linking it to a balance of probability (ought) from a reasonable person test creates confusion and room for a number of different interpretations of what is a private communication.

What is considered implied consent?

[5] Refer to the Parliamentary Counsel Office's drafting guidance: http://www.pco.parliament.govt.nz/clear-drafting/

6.12. Neither the definition, nor the Act, is clear on what constitutes 'implied consent' of someone who is party to a private communication. If a service provider's terms and conditions or End User Licensing Agreement includes reference to providing information to government agencies (and or law enforcement agencies), does that mean that there is implicit consent? What if T&Cs include reference to packet capture or deep packet inspection for security and network protection purposes?

The definition opens the possibility of different levels of protection based on knowledge or mental state.

6.13. We think that as well as being unclear and poorly worded, the definition could also create different levels of legal protection for New Zealanders with different levels of 'Internet savvy' or security concerns.

6.14. For example, take two members of InternetNZ:

a) one uses PGP-encrypted email, has kept abreast of the various leaks and publication of government surveillance and capturing of Internet-traffic by the Five Eyes partners

b) the other member has not taken these steps to build a field of knowledge about surveillance and security.

6.15. Does this mean that our first, more security conscious member is more likely to reasonably conclude, or suspect, that all of her encrypted messages are being intercepted? If so, could that mean that they are no longer considered private communications and could be intercepted by intelligence agencies without the need for a warrant?

6.16. One further, more troubling, implication would be that the existence of New Zealanders with this level of expectation of interception could be used to create an opportunistic interpretation that, all (or the majority of) communications are not private and are therefore not protected from unwarranted interception.

Our position on the definition of private communication

6.17. The inclusion of an individual's anticipated expectation of interception, the lack of clarity about who and what is party to a communication, conflation of explicit and implicit consent all combine to make a definition that is:

a) not understandable
b) is not easy to use
c) is inaccessible for a lay reader.

6.18. These three tests (understandable, easy to use, accessible) are the components of the Legislation Advisory Committee's standard for high quality law. Given the importance of the definition of a private communication to upholding New Zealanders rights against unreasonable search and seizure, this term should crystal clear to all readers.

6.19. Simply put, the definition of private communication is unclear, inadequate, potentially inconsistent in its application to individuals, and should be changed to better align with standards for good law in New Zealand. We would welcome any future opportunity to work with you, your officials and our members to provide alternative drafting for the definition of private communication.

InternetNZ

Should metadata be protected as well as content? (question 22)

6.20. Question 22 of your consultation document asks about private communication and whether the metadata of a private communication should be protected as well as the content.

6.21. Metadata is ever present in Internet-based communication and activity. As well as our browsing habits, our PCs and laptops, tablets, phones, cars and smartwatches produce metadata showing where we go, how we get there, our walking patterns, our daily lifestyle, who we call, what shops we visit and so forth. Metadata can be a hugely powerful resource for identifying individuals, understanding what they do, where they go and who they interact with. New developments in cloud computing and so-called "Big Data" analysis means that evermore meaning can be derived from what previously would simply have been masses of digital data.

6.22. For example, researchers at Stanford University had people take part in a study by downloading an app that harvested metadata for research analysis. Their results, which they have blogged about, help demonstrate that telephone metadata can be very informative and used to infer very sensitive information about someone's life. For example, they were able to infer information about whether an individual (or someone close to them) had multiple sclerosis and information indicating another participant was growing illegal drugs.[6]

6.23. It is this analytical power that makes metadata a desirable information source for intelligence and law enforcement agencies.

6.24. We consider that the metadata of private communications should be protected in the same way as the content of a private communication. We think that bulk metadata should not be generally available to intelligence, or law enforcement agencies.

[6] http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata

InternetNZ

About InternetNZ

A better world through a better Internet

InternetNZ is a voice, a helping hand and a guide to the Internet for all New Zealanders. It provides a voice for the Internet, to the government and the public; it gives a helping hand to the Internet community; and it provides a guide to those who seek knowledge, support or any other method of benefiting the Internet and its users.

InternetNZ's vision is for a better world through a better Internet. To achieve that, we promote the Internet's benefits and uses and protect its potential. We are founded on the principle of advancing an open and uncaptureable Internet.

The growing importance of the Internet in people's everyday lives means that over the last twelve months we have significantly reoriented our strategic direction. The Internet is everywhere. We are a voice for the Internet's users and its potential to make life better.

InternetNZ helps foster an Internet where New Zealanders can freely express themselves online – where they can feel secure in their use of the Internet. We foster an Internet where a start-up can use the web to develop a presence and customer base for a new product, and we foster an Internet where gamers can get online and battle it out.

We work to ensure this Internet is safe, accessible and open.

The work we do is as varied as what you can find on the Internet.

We enable partner organisations to work in line with our objects – for example, supporting Internet access for groups who may miss out. We provide community funding to promote research and the discovery of ways to improve the Internet. We inform people about the Internet and explain it, to ensure it is well understood by those making decisions that help shape it.

We provide technical knowledge that you may not find in many places, and every year we bring the Internet community together at NetHui to share wisdom, talk about ideas and have discussions on the state of the Internet.

InternetNZ is the designated manager for the .nz country code top-level domain and represents New Zealand at a global level through that role.

InternetNZ is a non-profit open membership incorporated society, overseen by a council elected by members. We have two wholly owned subsidiaries that ensure that .nz is run effectively and fairly – the Domain Name Commission (DNC) develops and enforces policies for the .nz domain name space, and .nz Registry Services (NZRS) maintains and publishes the register of .nz names and operates the Domain Name System for .nz

For more information visit: https://internetnz.nz/about-us/internetnz-group