InternetNZ

New Zealand Intelligence and Security Bill

Submission to the Foreign Affairs, Defence and Trade Committee

7 October 2016

Introduction

InternetNZ appreciates the opportunity to provide the Foreign Affairs, Defence and Trade Committee with our thoughts and views on the Intelligence and Security Bill 2016.

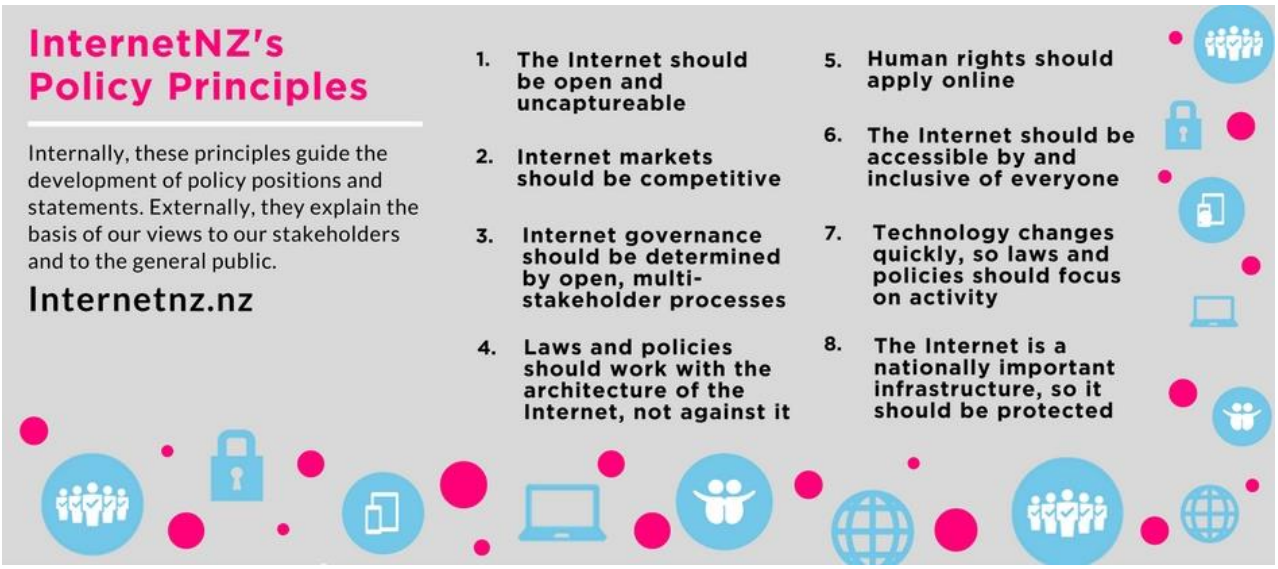
We would like to appear before the Committee to discuss the recommendations we make in this submission and answer any questions you may have.

We are committed to an open and uncapturable Internet

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.

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.

Figure one: InternetNZ's policy principles



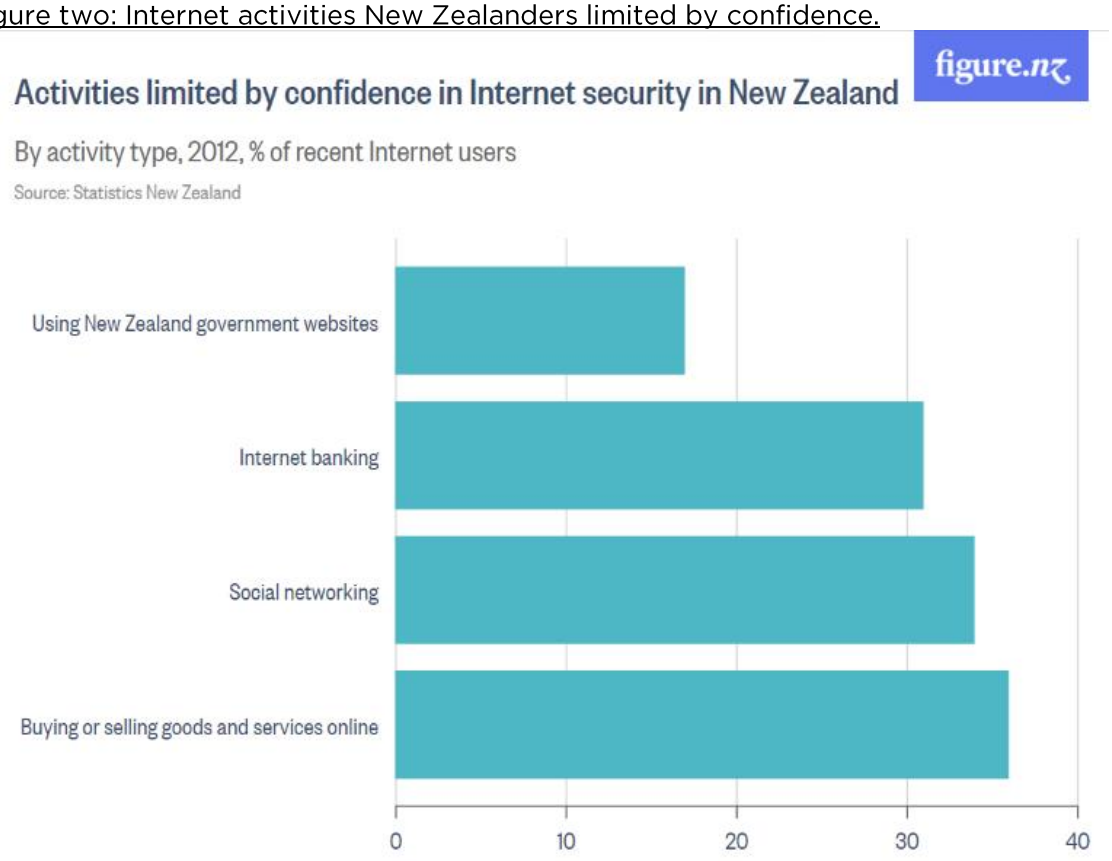
Executive Summary

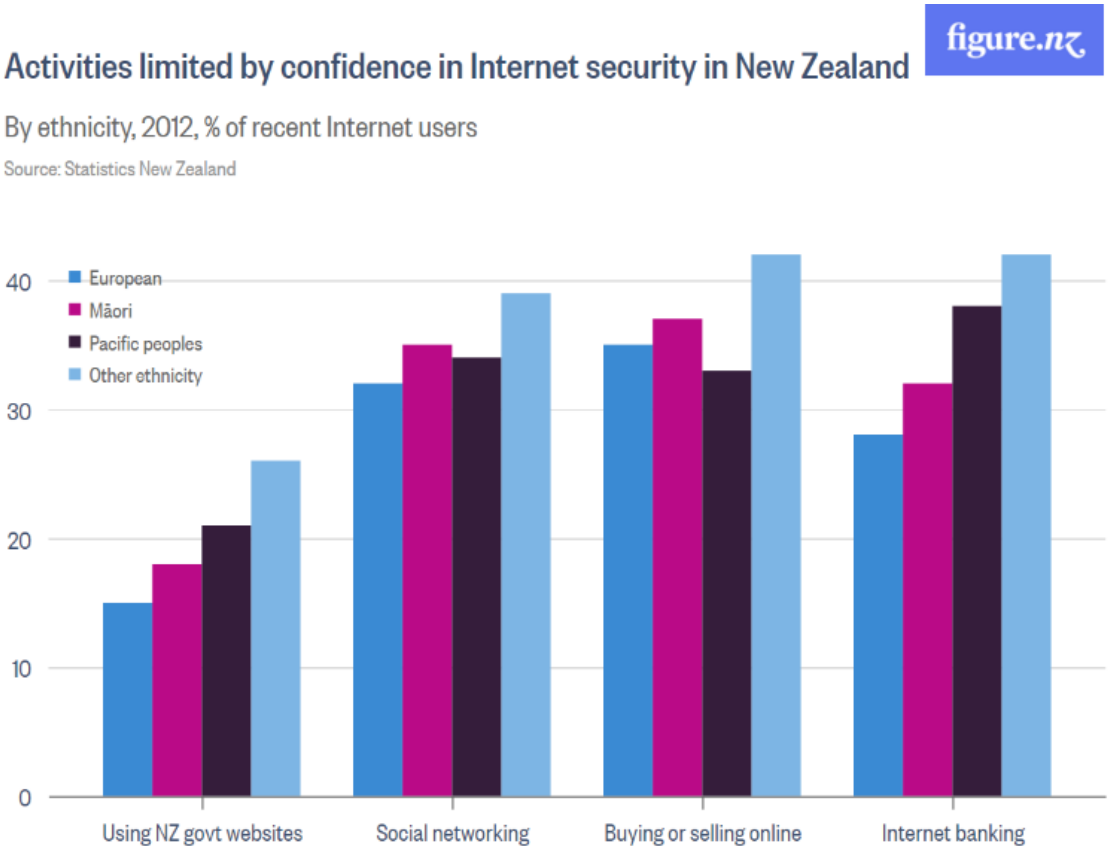
Surveillance - government or corporate - is of concern to users of the Internet. Surveys have shown that New Zealanders do care about their privacy and are worried about government's monitoring their Internet use. For example:

- the World Internet Project 2015 found that 68% of New Zealanders actively try to protect their online privacy;
- the World Internet Project 2015 found that 32% are concerned about Government monitoring their Internet use;
- an Amnesty International survey found that 63% of New Zealand respondents were opposed to New Zealand government surveillance of the Internet and phone use.

These concerns are having a real impact on chilling New Zealanders perceptions on whether and how they may use the Internet. For example, figure two, taken from our 2016 State of the Internet report (https://stateoftheinternet.nz) shows how New Zealanders avoid using the Internet for commercial and social purposes due to a lack of confidence in Internet security.

Figure two: Internet activities New Zealanders limited by confidence.





This legislation is an opportunity to place New Zealand's legal framework governing the work of the security services beyond doubt. Consistent with the government's position that mass surveillance is not currently undertaken, this legislation should remove any ambiguity about whether such activity would be lawful if done.

In our view, taking an unambiguous approach to this draft legislation would be the best way to help build the confidence of New Zealanders in the platform. Fears of surveillance could be shown to be ruled out by the law. It is this opportunity that guides our interest in this matter.

We have identified a number of areas of concern that, as an Internet focussed organisation, we think Parliament should address in order to maintain an appropriate balance between liberty, security and protecting the Open Internet.

1. We support the Bill's increased oversight of the NZSIS and GCSB. The oversight and accountability processes set out in the Bill are a commendable improvement on current law.
2. The definition of national security is too broad. As the definition that constrains the GCSBs ability to spy on New Zealanders, this is particularly concerning in the context of the chilling effect of public utilisation of the Internet. We recommend a definition that is narrower in scope and more consistent with the Bill's sections relating to purposes and objectives of the intelligence agencies.
3. The focus on only warranting 'unlawful' activity goes against the Reviewers' recommendations and maintains the reliance on a flawed and self-defeating definition of private communications to protect New Zealanders communications from unwarranted interception.
4. The rules and requirements around incidentally and collaterally obtained information should be amended to ensure that information obtained through protective security roles (e.g. the NCSC's cybersecurity role) cannot be used for intelligence or shared for law enforcement purposes. This hits directly to the heart of New Zealanders' protections against unreasonable search and seizure and protections against unwarranted search.
5. The definition of serious crime has a threshold that is too low and out of step with New Zealand criminal law.
6. We think the Bill should be drafted to explicitly prohibit mass surveillance. The current government does not do it, nor has previous governments - we think that any future government or agency staff should be legislatively barred from undertaking mass surveillance of New Zealanders.
7. We also raise a small number of more detailed amendments that would support greater confidence and accountability of the intelligence agencies.

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

We welcome the Bill's improved oversight and accountability measures

Before we set out the concerns that we have with the Bill, we want to confirm that we welcome and support the increased oversight and accountability measures that the Bill introduces. These include:

- the improved powers and role for the Inspector-General of Intelligence and Security
- the agencies being brought further into the Public Service under the Privacy Act's privacy principles
- a single, clear warranting system that clearly sets out what is permitted, and when
- a clear role for the Attorney-General, rather than the Minister responsible for the agencies.

These improvements, combined with our recommended amendments would enable the Bill to place New Zealand's legal framework governing the work of the security services beyond doubt, and build New Zealanders confidence in the Internet as an open and uncapturable platform.

Robust definitions and Parliamentary intent

One particular issue that we want to raise with the Committee relates to 'valid interpretations' versus parliamentary intent. In most situations, agencies follow purportive interpretation and officials will consult Hansard, and Select Committee reports to try and understand what was intended by Parliament if there are questions about how to interpret a piece of law.

Intelligence agencies are different. We can, and should, expect intelligence agencies to use law to its fullest to protect the nation. However, to ensure that New Zealanders are not deterred from using the Internet to its fullest, through fear, we need crystal clear law setting out what agencies are, and are not, permitted to do.

We suggest that, rather than thinking about what you think a section in the Bill is supposed to mean, instead think about what it could be read to mean? The Bill's definitions should be clear and unambiguous, with very limited capability for organisations to make an error when interpreting it. It is with this in mind that we have reviewed the Bill.

A better definition of national security is needed

The Bill's definition of national security is a critical component of a number of aspects of the Bill as it is central to both the purpose of the Bill (section 3) and the objectives of the agencies (section 11). But, more importantly, as the Intelligence and Security Act, the Bill's definition of national security will bind our intelligence agencies and the activities they will be permitted to undertake in relation to New Zealanders. Any 'unlawful' activity they seek to do in relation to a New Zealander will require a tier 1 warrant, and thus will need to pertain to a national security matter.

As the primary legislative definition that dictates the scope of GCSB and NZSIS action in relation to Internet surveillance or interception, we think this definition is critically important and needs to be tightly, and robustly defined with little room for confusion or misinterpretation.

Unfortunately, the current definition is flawed in a number of ways.

1. It includes "potential threats": this is a very broad concept that potentially creates an exceptionally low bar for spying on New Zealanders.
2. It includes international security: we fail to see how international security could be considered as a part of the definition of national security when international relations and well-being is separated from the concept of national security.
3. The section that relates to critical infrastructure is overly broad and unclear.
4. It includes threats to the life and safety of New Zealanders overseas: the health of individuals, not situated in the country cannot be credibly considered national security matters. section 17 adequately provides for these situations.
5. It includes economic security: the economic well-being of New Zealand is already a separate concept from national security. We do not see the need to include economic security in the concept of national security.

Alternative definitions

The fact sheets the Government released at the same time as the Bill and the Cabinet papers, set out an alternative definition for national security to that of the reviewers.

> *The proposed activity is necessary for the collection of intelligence relating to one or more of the following activities in New Zealand or overseas:*
>
> *a) Terrorism or violent extremism;*
> *b) Espionage or other foreign intelligence activity;*
> *c) Sabotage;*
> *d) Proliferation of weapons of mass destruction (chemical, biological, radiological, or nuclear weapons);*
> *e) Activities which may be relevant to serious crime and involve:*
> *i. the movement of money, goods or people;*
> *ii. the use or transfer of intellectual property;*
> *iii. the improper use of an information infrastructure;*
> *iv. damage to New Zealand's international relations or economic security;*
> *f) Threats to, or interference with, information (including communications) or information infrastructure of importance to the Government of New Zealand;*
> *g) Threats to international security;*
> *h) Threats to New Zealand government operations in New Zealand or abroad;*
> *i) Threats to New Zealand's sovereignty, including its territorial or border integrity and system of government; and*
> *j) Threats to the life or safety of New Zealanders.*

We consider this alternative definition to also be overly broad and contain components that should not be included, as well as some that create considerable room for interpretation.

1. Infringement of intellectual property is not a serious crime - it is predominantly a civil matter. How would agencies interpret the scale and severity of an intellectual property infringement to require their intervention, or would someone using BitTorrent, sharing important IP simply be enough of a "potential threat" to rationalise an intelligence operation?
2. Additionally, "improper" use of a network does not appear to be a very high standard at all.
3. International security is not national security (it relates to security issues of a global scale or security issues between nations)

In short, the alternative definition suggested by officials is also subject to many of the same criticisms of the Bill's definition.

We think the Bill should have a robust, and well worded definition that cannot be interpreted in a way that widens the scope for intelligence agencies to spy on New Zealanders. We propose a new definition of national security, one that represents a more tightly scoped version of officials' alternative definition:

Our proposed definition marked up against officials' proposal	Our proposed definition
*In this Act, **national security**, means that t~~T~~he proposed activity is necessary for the collection of intelligence relating to one or more of the following activities ~~in New Zealand or overseas~~:* a) *Terrorism or violent extremism in New Zealand;* b) *Espionage or other foreign intelligence activity in New Zealand, or against New Zealand;* c) *Sabotage in New Zealand or against New Zealand Government operations;* d) *Proliferation of weapons of mass destruction (chemical, biological, radiological, or nuclear weapons);* e) ~~*Activities which may be relevant to serious crime and involve:*~~ ~~i) *the movement of money, goods or people;*~~ ~~ii) *the use or transfer of intellectual property;*~~ ~~iii) *the improper use of an information infrastructure;*~~ ~~iv) *damage to New Zealand's international relations or economic security;*~~ f) *Threats to, or interference with, New Zealand's critical national infrastructure* ~~*information (including communications) or information infrastructure of importance to the Government of New Zealand*~~*;* g) ~~*Threats to international security;*~~ h) *Threats to New Zealand government operations in New Zealand or abroad;* i) *Threats to New Zealand's sovereignty, including its territorial or border integrity and system of government; and* j) ~~*Threats to the life or safety of New Zealanders.*~~ k) *threats that may cause serious harm to the safety of a population of another country as a result of unlawful acts by a New Zealander that are ideologically, religiously, or politically motivated.*	*In this Act, **national security**, means that the proposed activity is necessary for the collection of intelligence relating to one or more of the following activities –* a) *terrorism or violent extremism in New Zealand;* b) *espionage or other foreign intelligence activity in New Zealand, or against New Zealand;* c) *sabotage in New Zealand or against New Zealand Government operations;* d) *proliferation of weapons of mass destruction (chemical, biological, radiological or nuclear weapons);* e) *threats to, or interference with, New Zealand's critical national infrastructure;* f) *threats to New Zealand government operations in New Zealand or abroad;* g) *threats to New Zealand's sovereignty, including its territorial or border integrity; and* h) *threats that may cause serious harm to the safety of a population of another country as a result of unlawful acts by a New Zealander that are ideologically, religiously, or politically motivated.*

This definition addresses all of the traditional concepts of national security as it relates to the tasks of the NZSIS (e.g. espionage, sabotage, terrorism and anti-proliferation), it addresses counter-intelligence operations, and threats to New Zealand's way of life and population. It also recognises the role of the intelligence agencies to protect other countries from ideologically motivated New Zealanders who may wish to do them harm.

Private communications and interception warrants

In its policy decisions about the Bill, the Government made a considerable deviation from the Independent Reviewers' recommendations and decided that only unlawful activity would require a warrant, rather than all intelligence activity. One of the consequences of this approach is that the Bill has retained a definition of a private communication (interception warrants are required for the interception of private communications).

Unfortunately, the Bill continues the existing flawed and self-defeating definition of private communication from the GCSB Act 2003. The existing definition of private communication (used in the GCSB Act and the Crimes Act) has been subject to considerable commentary and criticism since 2003. This includes:

1. the Law Commission recommended a shorter, single 'reasonable expectation of privacy' test for private communications in stage three of its review of privacy law in 2010
2. the Legislation Advisory Committee advising the Government that the definition of private communication is flawed in 2013[1]
3. the New Zealand Herald publishing an op-ed on the inadequacy of the definition of private communication and the risks it creates[2]
4. the Cabinet papers authorising the Bill stated that "*the definition of what a private communication is in itself a quagmire*" (Cabinet Paper 1, paragraph 52).

As the Law Commission pointed out in its review of surveillance law:

> *"A communication can be rendered non-private and therefore susceptible to lawful interception if there is a sufficient likelihood that the communication may be intercepted. …we think it is unsatisfactory that the scope of the interception offence can turn on the likelihood of interception, an activity which the offence provision is purporting to regulate."*[3]

The Bill's definition has minor wording changes from the GCSB Act but it is effectively the same in that the same tests and concepts are used that create complications. In our submission to the Independent Reviewers, we spelt out a number of issues with the definition of private communication that we think needed to be addressed (a copy of the relevant part of our submission is attached as **Appendix A**).

To summarise, 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:

1. not understandable
2. is not easy to use
3. is inaccessible for a lay reader.

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 and not subject to any confusion or "legally valid readings" that could enable the warrantless interception of private communications.

---

[1] LAC letter to Prime Minister on GCSB Amendment Bill 2013 https://www.parliament.nz/resource/en-nz/50DPMCISC_SUB_00DBHOH_BILL12122_1_LAC1/ae2cd10e7ad8f8cecff786ecae49200e29e8110d

[2] Denis Tegg op-ed: http://m.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11308965

[3] Law Commission's *Invasion of Privacy: penalties and remedies*, 2010, paragraph 3.66

Maintaining the status quo definition as proposed in this Bill is the wrong approach. Its inclusion would inadvertently create an opening for the mass collection of communications or for mass surveillance and so would further reinforce the chilling effect on the use of the Internet already noted above.

Given the government's assurances that this activity does not occur, it would be preferable to resolve the definition so that the law is in line with the current approach. To put it another way, this definition is central to the question "does the law allow mass surveillance?" - and so it needs to be changed.

Our recommended approach

We recommend the Bill be amended to require a warrant in each instance or case where a communication (or class of communications) is intercepted, whether the communication is private or not (i.e. whether it would ordinarily be a lawful activity or not). Requiring a tier one warrant for intercepting any communications from a New Zealander would be in line with the report of the Independent Reviewers.

We think that this is the appropriate level of protection for communications interception on New Zealanders. We recommend that:

1. section 63(1)(b) should be amended to require an authorisation for “intercepting any ~~private~~ communication~~s~~ or class of ~~private~~ communications”
2. section 64(1)(b) should be amended to require an authorisation for “intercepting any ~~private~~ communication”
3. the Bill cross-reference the Telecommunications Act’s definition of a communication.

This proposed approach would be preferable to trying to find a workable definition of private communication and then requiring a warrant for the interception of a private communication (or classes of communications) for a number of reasons.

1. There is no already drafted alternative (e.g. one that relies on a single reasonable expectation of privacy test) that has been subject to analysis and comment from legal and civil liberties experts.
2. Any new definition inserted at this late stage would not be subject to a public engagement processes before being enacted.
3. A new definition could still contain unclear language, adding to the chilling effect the Bill would have on New Zealanders use of the Internet.

Unauthorised and incidentally obtained intelligence should be very tightly controlled

We have general reservations around information collected under specific functions being re-used for other purposes as incidentally obtained intelligence (despite not being related to the function for which it was collected), or the permissions that the Bill creates for the post-ante use of unauthorised intelligence in section 83.

We refer to the functions outlined in Part 2 sections 13 and 14. We would point out this actually includes Section 15 ‘information assurance and cybersecurity activities’, as that is referenced in Section 14(2)(a)(ii). Our reading of the Bill leads us to conclude that any information therefore collected under Project CORTEX or other NCSC activities will be treated as incidentally obtained intelligence as outlined in Part 4 section 47. We are concerned that parties interacting with NCSC or under project CORTEX may not be aware of the extended use of any data they share.

The Bill permits incidentally obtained intelligence to be shared broadly with:

1. any employee of the New Zealand Police:
2. any member of the New Zealand Defence Force:

3. any employee of the other intelligence and security agency:
4. any public authority (whether in New Zealand or overseas) that the Director-General considers should receive the information.

In addition, s83 sets out a process for the agencies to seek warrants to use already-obtained information about New Zealanders where they have previously obtained a lower-level warrant, presumably for a foreign-focused intelligence operation.

Intelligence agencies are given significant and invasive powers which, in many circumstances, breach New Zealanders protections relating to unreasonable search and seizure. The Bill's highly permissive framework enables the intelligence agencies to share information they acquire in their protective security roles with any public agency they see fit.

This permissive environment undermines New Zealanders confidence in the Internet and potentially undermines the benefits that we, as a society can gain from the Internet.

We recommend that the Committee places clear restrictions of the use of unauthorised intelligence, requiring it to be destroyed without recourse to post-ante warranting. This can be done by deleting s83(2) and 83(3).

We recommend that the Committee removes the ability for intelligence agencies to treat information obtained under their protective security roles (as set out in s14 and s15) as incidentally obtained intelligence. In order to preserve New Zealanders ability to trust and collaborate with protective security experts in the agencies, they need to have the confidence that information will not be misused for broader missions.

Serious Crime Definition

The circumstances under which incidentally obtained intelligence may be shared are also fairly broad. Of particular concern, under Part 4 Section 91(3)(A) incidentally obtained intelligence may be shared to assist in preventing or detecting serious crime in New Zealand or any other country.

However, we note that within this Act 'serious crime' is defined as any offence punishable by 2 or more years' imprisonment. We feel this far too low to be considered 'serious crime' and that these provisions would be best if aligned with other legislation - that is, if this were 7 years imprisonment or at the very least 5 years or more imprisonment.

a) A seven (7) year minima (potentially with some additionally specified crimes with lower imprisonment terms) would be consistent with the Search and Surveillance Act's restrictions on surveillance device warrants (see s45 of the Search and Surveillance Act 2012)
b) A five (5) year minima would be in line with concepts of serious crime used in statute about money laundering and the civil asset recovery regime.

We are not aware of any other New Zealand statute, or International treaty that New Zealand has signed or ratified, where the concept of "serious crime" is used to reference crimes that have a maximum imprisonment term of 2 years.

Prevention of Mass Surveillance

The Government says that it does not undertake mass surveillance of New Zealand or New Zealanders. The Factsheets that it published when the Bill was introduced make it clear that this statement has been confirmed by both the Inspector-General of Intelligence and Security, and the Independent Reviewers.

It is important to note that a reasonable interpretation of this legislation as drafted could still allow for the mass surveillance of New Zealanders as they use the Internet, or the mass collection of information about their Internet use.

We would prefer to see more explicit controls and limitations on this. We have already highlighted our concerns regarding incidentally obtained intelligence and its secondary usage. We also note there is potential for vast quantities of data to be gathered under activities covered in Sections 13 to 15 of Part 2.

We are also concerned that any activity that is 'lawful' (Part 2, Section 15(3)) doesn't require a warrant. This could potentially include data willingly shared in accordance with the Privacy Act Principle 11. Our concerns are heightened by the wording of Part 4 Section 83, which appears to offer various options for collecting unauthorised intelligence and then applying for the appropriate warrant after its collection (Section 83 sub-section(3)).

Taken together, it is arguable that this combination of matters would render the legislation enabling of mass surveillance programmes involving the Internet.

Therefore, we recommend that, given Parliament (and the Government) are committed to not enabling mass surveillance, then an additional section should be inserted into the Bill after section 22 (which deals with limitations on intelligence collection), clearly stating that the GCSB and NZSIS are specifically prohibited from conducting mass surveillance of New Zealand or New Zealanders or the mass collection of information that could be used for surveillance (mass or targeted) in future.

Minor issues

In our analysis of the Bill, we have also identified a number of more minor concerns that, if left, could undermine some of the Bill's important steps to bolster transparency and accountability.

Metadata should be explicitly included in a definition, or concept of data

One of the Independent Reviewer's recommendations that we most supported was their agreement that metadata should be treated the same a data (e.g. communication content), and subject to warranted access only. We recommend that, for the avoidance of doubt, the Bill be amended to explicitly include metadata in the definition of communication.

Protection of staff identity could interfere with protection security roles

Throughout the Act there are various protections relating to the identity of staff and employees within the agencies. This seems in some ways at odds with the more public facing activities outlined in Part 2, Sections 13 to 15. Protecting the identity of staff and employees engaged in covert activity makes sense. However, several staff are engaged in activities that involve interaction with members of the public and private sector. For example, almost every staff member of the National Cyber Security Centre would require special dispensation from the Director of the GCSB in order to do their job. We suggest that staff in protective security roles are excluded from these provisions.

Withholding information from Annual reports

Sections 179 and 180 contains grounds under which the Minister responsible may withhold information from the report to House of Representatives. These grounds are similar but not the same as the Official Information Act (the OIA). We feel that using and referencing the OIA for grounds to withhold would make more sense. In addition, the OIA contains the appropriate checks and balances whereby the Ombudsman would be able to investigate and review

decisions to withhold information from an annual report. The Bill does not appear to have the same mechanisms.

We suggest that either:

a) these provisions are removed and instead the agencies and ministers rely on OIA to withhold sensitive information
b) the Bill be amended to copy the OIA's provisions (see s6 of the OIA) relating to national security reasons to withhold information, and include an ability to appeal to the Ombudsman for a review.

Some NZ-based organisations cannot complain to the Inspector-General

It appears there are limitations regarding complaints which could have a chilling effect on Internet-related companies.

Part 6 Section 134 only allows for complaints from a 'New Zealand person'. A number of Internet related companies that operate in New Zealand are therefore unable to complain if they feel activities of an Intelligence and Security agency have impacted them in some way. This also applies to a number of New Zealand organisations that could be considered Critical National Infrastructure operators or Network Operators under the Telecommunications Interception and Security Act (TICSA).

Given New Zealand's high rate of foreign-owned companies (including the majority of our banking sector and many of our ISPs), it would seem prudent to enable a foreign-owned business that is operating in NZ (and has a relationship with the agencies either through protective security roles or statutory obligations) to make a complaint to the Inspector-General about an intelligence agency, just like any other organisation or person in New Zealand.

Jordan Carter
Chief Executive
InternetNZ

About InternetNZ

A better world through a better Internet

InternetNZ's vision is for a better world through a better Internet. We promote the Internet's benefits. We protect its potential. And we focus on advancing an open and uncaptureable Internet for our country.

We provide a voice for the Internet in New Zealand and work on behalf of all Internet users across the country.

We are the designated manager for the .nz Internet domain. And through this role we represent New Zealand at a global level.

We provide community funding to promote research and the discovery of ways to improve the Internet. We inform people about the Internet and we ensure it is well understood by those making decisions that help shape it. Every year we bring the Internet community together at events like NetHui to share wisdom and best practice on the state of the Internet.

We are a non-profit and open membership organisation.

Be a member of InternetNZ and be part of the Internet community. You can keep a close watch on the latest tech and telecommunications developments and network with other like-minded people at cool events. Being a member of InternetNZ only costs $21 per year. Find out more at internetnz.nz/join

For more information about InternetNZ, visit internetnz.nz

Appendix A

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
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.4 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?

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?

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

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.