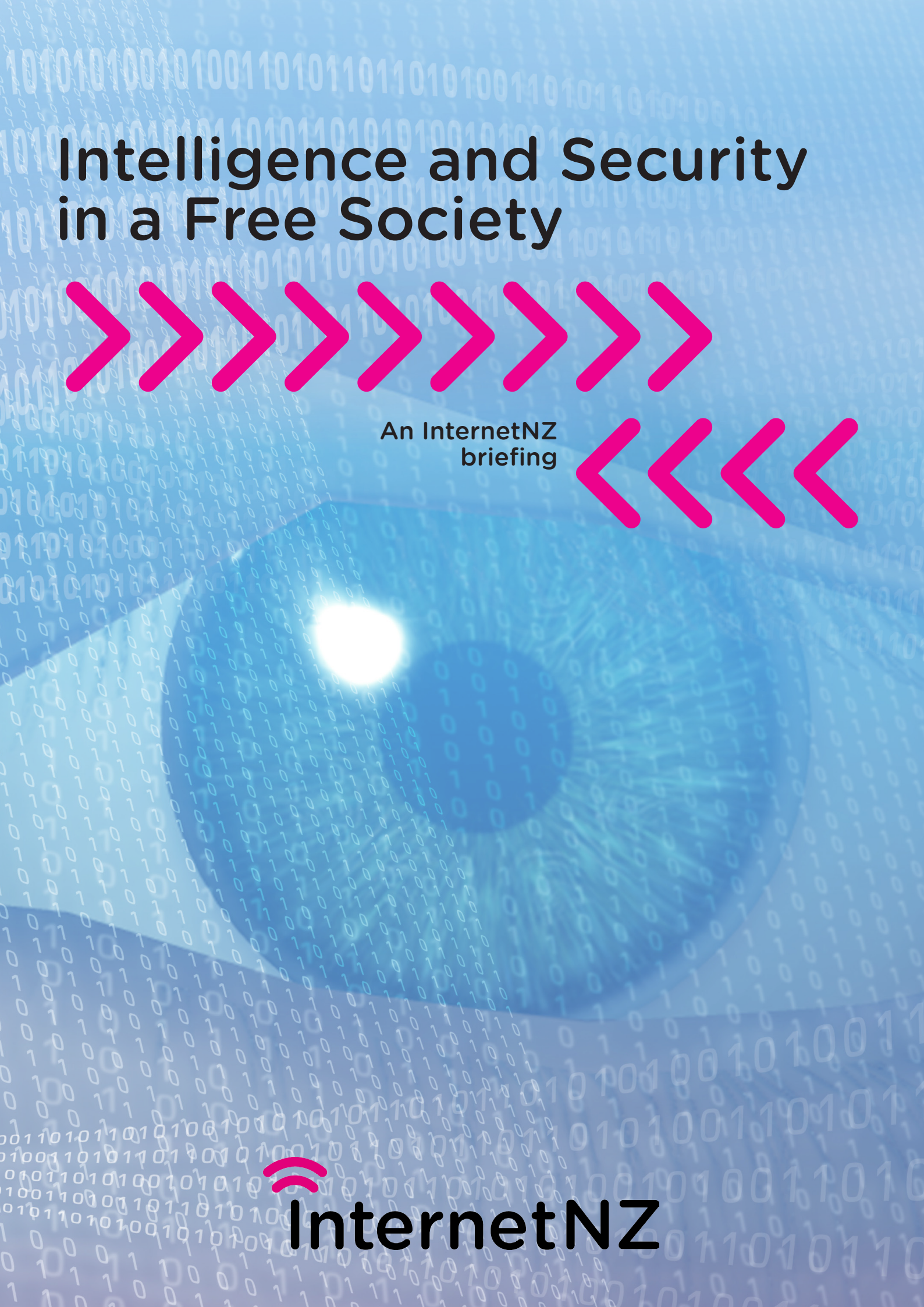
# Intelligence and Security in a Free Society

An InternetNZ briefing



InternetNZ

**On 9 March 2016, The Independent Reviewers of Intelligence and Security released their report on New Zealand's intelligence agencies, titled Intelligence and Security in a Free Society.**

**So what is this review, what does the report say and what does it mean for the Internet community?**

**This short briefing gives you a heads-up on what the review is, what we like, what we don't like, our thoughts on some process issues, and ultimately what the review and its proposals would mean for New Zealanders.**

# At a glance

The report is a mixed bag. The reviewers acknowledge human rights, and the need to keep New Zealand a free and open society. Unfortunately, those priorities, and the consequences for liberty, freedom and an open and uncapturable Internet are not reflected in the recommendations.

The report's main points include the following.

1. The report has some great proposals on better oversight and accountability for the GCSB and the New Zealand Security Intelligence Service. These are welcome and sorely needed changes.
2. The report proposes that the GCSB be able to spy on New Zealanders. We think that's a bad idea - we don't let the army be our police, why would we let a foreign-intelligence organisation spy on us?
3. The proposed definition of national security is supposed to limit the GCSBs ability to spy on New Zealanders, but it is broad and open to multiple interpretations. It will not constrain spying on New Zealanders and their Internet communications and it needs to be rewritten.
4. We are no closer to a good, easy to understand definition of what a private communication is. The reviewers have recommended a new legal approval system that would require authority for all spying, so they don't need a private communication definition. However, the same definition is in other pieces of law and we'd like clarity on what is, and what isn't a private communication in New Zealand law.
5. The reviewers have correctly stated that agencies access to communications metadata should be subject to the same authorisation as the content of communications. We couldn't agree more.

# What is the review?

In May 2015, the Attorney-General appointed Hon Sir Michael Cullen (former Deputy Prime Minister and Chair of NZ Post) and Dame Patsy Reddy (an experienced barrister and solicitor, Company Director and law lecturer who has led performance reviews of government departments) to review New Zealand's Intelligence Community.

Called the Independent Review of Intelligence and Security, or IRIS for short, Sir Michael and Dame Patsy reviewed the NZ Security Intelligence Service (NZSIS) and Government Communications Security Bureau (GCSB), sought public submissions and reported back to the Government on 9 March 2016.

You can read a copy of their report here:

https://consultations.justice.govt.nz/independent/iris

# Why do we care?

**Because human rights apply online, because the Internet is full of potential and this potential should be protected.**

The GCSB, like other signals intelligence agencies uses the Internet to spy on people. Research shows that we change our behaviour online when we know that someone is watching.

The Internet is a powerful tool to create a better world, but we believe this requires a better, open and uncapturable Internet. So yes, we care passionately about the GCSB's powers to spy on New Zealanders' use of the Internet.

# Why should you care?

Because the Internet is yours. It's potential and its future is in your hands. And because we know that, thanks to Amnesty International's surveys, nearly three times more people would oppose New Zealand government surveillance of the Internet than those that approve it (63% vs 22%).[2]

Recent research has also shown that people really do silence their own minority opinions when they know that their online behaviour is being monitored by government agencies. The author of that research put it like this: [3]

*"The adoption of surveillance techniques, by both the government and private sectors, undermines the Internet's ability to serve as a neutral platform for honest and open deliberation. It begins to strip away the Internet's ability to serve as a venue for all voices, instead catering only to the most dominant."*

**New Zealand's free society is your society. How much you are spied on should be a debate that you are involved in.**

1. You can read our submission on our website: https://internetnz.nz/content/submission-independent-review-intelligence-and-security
2. https://www.amnesty.org.nz/new-zealanders-part-global-opposition-usa-big-brother-mass-surveillance
3. Stoycheff, E. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring Journalism & Mass Communication Quarterly, first published on March 8, 2016 https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/

# What we like

**At 180 pages long, it's not surprising that there's parts of the report we really like. This section sets out the parts of the report we support and welcome.**

### Support for human rights and an open society

The title of the report puts freedom front and centre. The report talks at the very beginning of New Zealanders' rights to freedom and liberty. We're not sure that this stated principle has been adequately flowed through to the rest of the report and its recommendations, but it's still a good thing to see a security and intelligence review clearly state what the goal and purpose of our national security apparatus is and how it is supposed to protect our freedoms, liberties, democracy and ways of life.

### Increased accountability and oversight

**The report contains a number of recommendations that will increase accountability, oversight and the ability for New Zealanders to understand how the intelligence agencies operate and what they are legally allowed to do.**

These improvements include:

- a single warrants system will make it clearer how much surveillance these agencies are doing
- multiple judicial commissioners who sign off all warrants and authorisations (some of whom could be currently serving Judges)
- a larger Parliamentary Intelligence and Security Committee with a broader role would generate stronger political oversight
- bringing the agencies into the Public Service to bring their organisational and ethical frameworks into line with the country's expectation that they are fair, impartial, responsible and trustworthy.

### A strengthened, and more independent Inspector-General

The Inspector-General of Intelligence and Security is the main watch-dog of the intelligence agencies. The reviewers have recommended strengthening the Inspector-General's role, powers, ability to investigate agencies operations and the independence of the Inspector-General from Ministers. This is great and a strong, independent watchdog is a critical part of the checks and balances that intelligence agencies should operate under.

### A clear role for the Attorney-General

The Attorney-General is the chief law officer of the Crown. The reviewers have recommended that the Attorney-General, rather than the Minister responsible for the NZSIS and the GCSB, should be the politician that signs off intelligence agency warrants alongside a Judicial Commissioner. This strikes us as a sensible and useful separation of Ministerial powers and responsibilities and introduces another potential check and balance against agency overreach. But it will only be a meaningful separation if the Attorney-General and the Minister responsible for the agencies are different people.

### All surveillance must be authorised

The proposed tiered authorisation model would mean that all surveillance and intelligence gathering would be authorised and subject to clear oversight around what work is carried out under those authorisations.

**Accessing private information, surveilling people in public places and other activities that are currently done without authorisation would require authorisation. That's a good thing.**

We also like that, linked to this always have authorisation policy, is the concept of a 'review warrant' where any incidentally obtained intelligence about a New Zealander would require a tier one warrant to keep and access (otherwise it would need to be destroyed). Again, that would, in theory, increase the protections around intelligence agencies accessing our information and surveilling us.

### Metadata is data

The reviewers deserve a strong round of applause here.

They've recognised that metadata is a powerful analytical and surveillance tool and recommended that the collection of metadata should be subject to the same restrictions as content. We think this will be even more important as intelligence agencies begin to lose the ability to access content and will need to rely even more heavily on meta-data.

This recommendation is excellent news and we certainly hope the Government acts on it.

### A simpler legal framework

**A single warranting system with a single statutory framework will make it less likely for agencies to misread the law.**

It will also mean it's less likely for people to give them the benefit of the doubt if they do step outside the law. This is also useful for New Zealand's Internet service providers and our tech sector.

The laws that govern how the Government can get information from New Zealand organisations will be simpler and easier to learn.

# What we don't like

**While there are plenty of things we like in the report, there are also a number of recommendations and parts of the report that we are concerned about. Below are the things we think are the most problematic.**

### The GCSB will be spying on us

The idea that the GCSB will be deployed to spy on New Zealanders more is a particularly worrying aspect of these recommendations. The main rationale for this appears to be that the GCSB has more modern tools than the NZSIS and law enforcement agencies like New Zealand Police or the Customs Service, and that replicating this capability in those other agencies would be wasteful.

These modern tools have been characterised in the media as "hawkeye" or "snicko." Hacking New Zealanders phones, computers and routers to turn them into surveillance devices, or installing surveillance equipment inside commercial equipment are all capabilities the GCSB and its 'Five Eyes' allies have. These are highly invasive tools and technologies, built up over decades of foreign intelligence operations, that dramatically increase the ability of the GCSB to invade our privacy.

The case certainly has not been made as to why New Zealanders should accept the significant increase in the pervasiveness of domestic state surveillance, which is exactly what allowing the GCSB to spy on New Zealanders achieves. We are all constrained in understanding what the scope of this activity could be as we don't have visibility of the full range of technologies and methods that could be deployed in this regard. With that in mind we think, as a start, if the GCSB is going to be able to spy on New Zealanders, they should be constrained to passive, data-based warrants, as opposed to opening up their full suite of foreign intelligence tools to be used on us (the people they work on behalf of).

A similar distinction exists between police and military. We don't let the New Zealand Defence Force do the job of police at home. Instead, the police operate in line with domestic law while they enforce it. The military, however, operates under a different set of rules - International Law. That's always been the same rationale for the separation between domestic intelligence and foreign intelligence. Foreign intelligence agencies operate under different rules, cultures and expectations. Turning that external eye inward, without a solid case for why, is something we find concerning.

http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html
http://leaksource.info/2013/12/30/nsas-ant-division-catalog-of-exploits-for-nearly-every-major-software-hardware-firmware/

**The definition of national security is no constraint on spying**

The definition is a laudable academic approach to reflecting the way New Zealand has thought about national security as a broad range of concerns.

## New Zealand's 'all-hazards' approach has been followed too closely.

The reviewer's proposed definition for national security is set out below:

National security means the protection against:

- threats, or potential threats, to New Zealand's status as a free and democratic society from:
  - unlawful acts, or
  - foreign interference
- imminent threats to the life or safety of New Zealanders overseas
- threats, or potential threats, that may cause serious harm to the life, safety or quality of life of the New Zealand population
- unlawful acts, or acts of foreign interference, that may cause serious damage to New Zealand's economic security or international relations
- threats, or potential threats, to the integrity of information or infrastructure of critical importance to New Zealand
- threats, or potential 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
- threats, or potential threats, to international security.

That seems like a laudable definition of national security. But we don't think it adequately constrains the GCSB from spying on New Zealanders. Concepts like "serious damage," "unlawful," or what constitutes a "potential threat to information critical to New Zealand" could be read widely and used to justify significant spying on New Zealanders.

The reviewers' proposed definition of national security means that the possible use-cases for Tier 1 warrants raises questions as to whether the GCSB could spy on New Zealanders in the following situations:

- a New Zealander defacing a US government website through the Internet
- a New Zealand registered charity criticises the Government's record on human rights (could be considered undermining international relations)
- a New Zealander points out negative effects of an international trade agreement
- a New Zealander plans to publish information showing negative environmental effects or business practices of a foreign controlled, multinational company.

## In summary, this definition is broad and open to multiple interpretations. Our analysis suggests that it will not adequately limit spying on New Zealanders and their Internet communications and it needs to be rewritten.

**'Private communication' is still not appropriately defined**

As we said in our submission - the current definition of private communication used in New Zealand statute is deeply flawed and needs to be changed. However, the reviewers are recommending a new process which does not rely on a definition of a private communication and they have not provided any commentary or recommendations on the definition. This was an important part of their Terms of Reference that they've failed to deliver.

A real opportunity for better law and a clearer right to privacy has been missed.

**Encryption portrayed as a bogeyman, rather than a protector**

Encryption was raised as a problem and linked to paedophiles and child sex offenders. But the report made little comment about the needs for encryption for agencies' protective security roles or how the GCSB recommends and requires robust encryption to protect New Zealand's classified material and sensitive information (e.g. health data and financial information).

**Encryption is a core Internet security technology and we all need it to use the full potential of the Internet.**

Hand-waving and pointing to the fact that encryption is used by criminals (who almost always leverage new technology faster than law enforcement) doesn't recognise the fact that it has innumerable positive applications. Encryption is at the core of how the Internet can work effectively as a means for secure, private communication.

**Little detail on the National Cyber Security Centre and its role**

This is the newest and most important part of the GCSB for New Zealand's protective security and receives very little consideration in the report. While not a core part of the terms of reference for the reviewers, protective security is a very important part of the agencies roles. We would've liked to see more detail about how the GCSB's protective security mission intersects with its intelligence mission and the tensions in balancing offensive and defensive capabilities within agencies.

# Process and principles

**Human rights: All talk, no walk?**

The review begins by recognising fundamental democratic freedoms. The new law it recommends would have as its purpose "the protection of New Zealand as a free, open and democratic society." In other words, the reason we have security and intelligence services is to protect our way of life, including our democratic freedoms. This is a useful framing. We could apply it to consider specific powers and practices, asking "overall, does this help or hurt our democratic way of life?"

Unfortunately, this question is not asked in the review. Despite dozens of mentions of "individual rights," there is no substantive discussion of how security and intelligence practices might help or hurt democratic freedoms. This is a massive missed opportunity. Whether a particular practice is justified depends on the costs (how much intrusion into rights?) and benefits (how much reduction in security risks?).

The review could have discussed hypothetical case studies, helping New Zealanders to understand why limits on democratic freedoms might be justified. Instead, justification is assumed.

We are not asking for perfection. It's as simple as this.

**When proposing practices which could limit our freedoms, the reviewers should 'show their working,' just like any high school student.**

**The reviewers engaged in limited community engagement**

**The reviewers consulted well with government and academia but their active engagement with civil society, business and the technical community was disappointingly limited.**

The review took almost a full year (May 2015 to March 2016) and there would have been ample opportunity to engage with a broader group of stakeholders such as the Telecommunication Carriers Forum, ISPANZ, the NZ Internet Task Force, the wider information security community, the Council of Civil Liberties, TUANZ, InternetNZ and TechLiberty. This is particularly disappointing given the focus of the report on living in a free society.

As an organisation that engages in a lot of multi-stakeholder processes and fora, we think this narrow engagement has meant the reviewers have denied themselves access to many viewpoints and opinions that could have tempered their thinking, analysis and helped create a better report.

**Re-recommending recommendations?**

Lastly, one slightly perplexing part of the report is the re-recommending of previous intelligence review recommendations. For example, the recommendation to fold the Combined Threat Assessment Group into the National Assessment Bureau was made in 2009, under this Government. If that didn't happen then (which it didn't), why was that not at least mentioned in this review? Why didn't the Government follow the previous advice on this point? The suggestion to create a National Intelligence and Security Advisor was also suggested in 2009 and, as far as we can tell, acted upon. The role of Director, Intelligence Coordination was created within the Department of Prime Minister and Cabinet (the role formerly held by Roy Ferguson) a few years ago, however, this role and function seems to have been ceased for some reason (otherwise, why is it being recommended again?).

While this isn't a core InternetNZ issue, it does make us wonder how many of these recommendations will be taken up, which will be ignored, or if some will be acted upon and then quietly walked back when no-one is watching.

# What happens next?

The Government will be considering the report, and we are assuming they will make a formal response, then the cogs will start turning on creating new laws.

Before policy decisions are made we want to talk more with you, the Internet community, to understand what your concerns are, what you think about increased surveillance and where the line should be to ensure we stay a free society. We want to facilitate a community discussion.

# Some questions we still have

- What are the actual security risks we face? After 180 pages of words we couldn't see a clear case made about why more security and spying is needed.
- What is the need for the GCSB to spy on New Zealanders? We can't see a case that's been made apart from 'security protects liberty, spying is good for security, replicating the GCSB's tools in the NZSIS is a waste of money and resources, therefore allowing the GCSB to spy on New Zealanders is good for a free society.' That seems like shaky intervention logic to us.
- If the GCSB must be allowed to spy on us, can we constrain the tools they can use on us?

**What questions do you have? Which recommendations did you like or not like?**

**Join the conversation and tell us what you think. We'll be using the hashtag #EyesOnNZ on social media.**

# About InternetNZ

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 uncapturable Internet for our country.

We provide a voice for the Internet in New Zealand. We lobby the government. And we give a helping hand to Internet users across the country.

We help to foster an Internet where you, as New Zealanders, can do things like:

- freely express yourself online
- feel secure and safe using the Internet
- use the web to help flourish start-up businesses and products
- watch your favourite shows with the rest of the world and battle it out with gamers

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 NetHui and other events to share wisdom and best practice on the state of the Internet.

We are a non-profit and open membership organisation.

Do you want to be part of the Internet community, vote on elections and stand for council? Or maybe you just want to keep a close watch on the latest tech and telecommunications developments and network with other like-minded people at cool events? You can become a member of InternetNZ from only $21 per year. Find out more about how you can belong here:

www.internetnz.nz/why-join-internetnz