

PRIVACY AND INTERNET FREEDOM

TABLE OF CONTENTS

1. **Summary**
2. **Problems Identified**
 - 2.1. **GCSB's role and powers**
 - 2.2. **Inadequate protection of rights**
 - 2.3. **Inadequate Internet freedom**
 - 2.4. **Inadequate implementation of Privacy Act changes**
3. **Relevant Data / Research**
 - 3.1. **Surveillance of New Zealand digital communication**
 - 3.1.1. Unlawful activities of the GCSB
 - 3.1.2. Lack of public trust in the GCSB
 - 3.1.3. NSA surveillance of NZ Internet traffic
 - 3.1.4. NZ participation in the global surveillance apparatus
 - 3.1.5. Metadata is personal
 - 3.1.6. Mass surveillance is ineffective
 - 3.1.7. Impact on innovation and jobs
 - 3.2. **Inadequate protection of rights**
 - 3.2.1. Bill of Rights Act is weak and ineffective
 - 3.3. **Internet freedom**
 - 3.3.1. Assessment of New Zealanders' Internet freedom
 - 3.4. **Privacy**
 - 3.4.1. Privacy as a human right
4. **Examples of Global Leadership**
 - 4.1. **Against surveillance of digital communications**
 - 4.1.1. International Principles on the Application of Human Rights to Communications Surveillance
 - 4.1.2. EU parliamentary inquiry into mass surveillance
 - 4.1.3. ECJ ruling on EU Data Retention Program
 - 4.2. **Protecting rights**
 - 4.2.1. Canadian Charter of Rights and Freedoms
 - 4.2.2. The charter of human rights and principles of the Internet
 - 4.2.3. Brazil's Marco Civil
 - 4.2.4. Sir Tim Berners-Lee
 - 4.3. **Internet freedom**
 - 4.3.1. The Icelandic Modern Media Initiative
 - 4.3.2. NETmundial

5. Policy proposals

- 5.1. Review surveillance laws
 - 5.2. Strengthen human rights protection
 - 5.3. Strengthen Internet freedom
 - 5.4. Implement Privacy Act reform
-

1. SUMMARY

Privacy and Internet freedom are at risk in New Zealand from mass surveillance by the Government and its allies. The Internet Party will remove the legal basis for mass surveillance, and review intelligence co-operation agreements.

We will ask the Law Commission to review the Bill of Rights Act (1990) to see if it is fit for a digital future. We want it elevated to superior legislation, so all laws would have to comply with its provisions.

We will pass legislation requiring due process before websites are taken down. A general safe harbour for Internet intermediaries will be provided to conditionally shield them from liability for users' actions.

2. PROBLEMS IDENTIFIED

2.1. GCSB's role and powers

The Government Communications Security Bureau (GCSB) has illegally spied on New Zealand citizens and permanent residents, and has not been held accountable for its unlawful activities.¹

Last year's amendment to the GCSB legislation allows the GCSB to undertake mass surveillance of New Zealand citizens and permanent residents legally.² It expanded the GCSB's role in domestic spying and economic matters. Furthermore, there remains inadequate and ineffective oversight of the surveillance activities of the GCSB.³

As part of the Five Eyes intelligence sharing arrangement⁴, the GCSB's systems are integrated with the intelligence agencies of the United States (US), the United Kingdom (UK), Canada, and Australia, rendering New Zealand without sovereign control over its surveillance intelligence. The GCSB is tasked by Five Eyes rather than working to protect the interests of New Zealanders. The Five Eyes arrangement reflects New Zealand's colonial past and does not take into account current and future interests with other countries.

¹ http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11116460

² <http://www.legislation.govt.nz/bill/government/2013/0109/13.0/DLM5177706.html>

³ <http://www.3news.co.nz/GCSB-oversight-inadequate-HRC-says/tabid/1607/articleID/304736/Default.aspx>

⁴ <http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>

In addition, last year's amendment to the telecommunications interception regime⁵ allows the government a backdoor to ICT providers in secret, allowing for direct access to data and undermining trust in New Zealand's ICT companies.⁶ It further provides for the GCSB to intervene in the design and equipment chosen by telecommunication providers in the name of protecting national security.

2.2. Inadequate protection of rights

New Zealand does not have a constitutional bill of rights. The Bill of Rights Act (1990) is weak and ineffective in practice, allowing the government to pass laws that contradict the Bill of Rights and the International Covenant on Civil and Political Rights.⁷

Unlike the Privacy Act, there has been no review of the Bill of Rights Act to ensure it is fit for a digital age and that it can respond to challenges faced by digital communications surveillance.

What is more, the Government has shown no political will to protect New Zealanders' data from surveillance by the US communications intelligence organisation, the National Security Agency (NSA), or protest about drone strikes against New Zealanders overseas.⁸

2.3. Inadequate Internet freedom

Revelations by US whistle-blower Edward Snowden demonstrated there is heavy interference by government agencies in the fabric of the Internet.⁹

Website hosts in New Zealand are able to arbitrarily take down websites and content in the absence of a legislative framework. This also makes them vulnerable to unfair informal pressure from investigative authorities, without judicial oversight or legislative sanction.¹⁰

There is no authorising or controlling legislation of the Internet filter run by the Department of Internal Affairs.¹¹ This means that a decision to expand from only blocking access to child exploitation material to blocking any class of websites is purely administrative, with no Parliamentary oversight or decision-making.

Further, there are no general legal protections available to Internet intermediaries from liability for their users' activities, posing a threat to freedom of expression online.¹² Intermediaries are neither liable for, nor specifically protected from, refusing to take action that infringes human rights, and information

⁵ <http://legislation.govt.nz/bill/government/2013/0108/latest/whole.html>

⁶ <http://www.nbr.co.nz/article/revealed-govt-plans-secret-orders-so-service-providers-under-spy-bill-ck-144562>

⁷ <http://www.legislation.govt.nz/act/public/1990/0109/latest/whole.html#whole>

⁸ https://www.youtube.com/watch?v=pkHAJ_UUmso

⁹ <http://www.theguardian.com/world/the-nsa-files>

¹⁰ <https://www.apc.org/en/irhr/i-freedom-nz/arbitrary-blocking#fn358988299534e671b375b0>

¹¹ <http://www.dia.govt.nz/censorship-dcefs>

¹² <https://www.apc.org/en/irhr/i-freedom-nz/intermediary-liability>



about actions taken or not taken is not readily available from Internet intermediaries operating in New Zealand.

2.4. Inadequate implementation of Privacy Act changes

The Law Commission has taken an extensive review of the Privacy Act to assess privacy values, changes in technology, international trends, and their implications for New Zealand law.¹³ Since the Law Commission submitted its final report in 2011, the government has selectively implemented recommended changes. This leaves unaddressed major suggested changes - such as greater powers for the Privacy Commissioner and mandatory reporting of security breaches leaking personal information.

3. RELEVANT DATA / RESEARCH

3.1. Surveillance of New Zealand digital communications

3.1.1. Unlawful activities of the GCSB

A review of the GCSB's operations (the Kitteridge Report) in response to illegal spying on Kim Dotcom found the GCSB had illegally spied on at least 88 New Zealand citizens and permanent residents.¹⁴ Furthermore, the report uncovered systemic problems within the GCSB that led to a lack of compliance with existing laws. Since the passing of the GCSB Bill in 2013, and despite promises of reform from the Prime Minister, the GCSB has even failed to accurately report its surveillance activities at a summary level.¹⁵

3.1.2. Lack of public trust in the GCSB

As a result of the GCSB's unlawful behaviour, public confidence in the agency is low. A poll conducted following readings of the GCSB Bill in Parliament showed that 75.3 percent of New Zealanders were concerned about expanding the powers of the GCSB.¹⁶

3.1.3. NSA surveillance of NZ Internet traffic

Revelations by Edward Snowden have demonstrated that the NSA practises bulk surveillance of global Internet traffic through programs such as Fairview, which targets traffic running through international fibre optic cables.¹⁷ With almost all of New Zealand's Internet traffic travelling to or from the US going via the Southern Cross Cable, mass surveillance of New Zealand traffic by the NSA is a fact.

¹³ <http://www.lawcom.govt.nz/project/review-privacy>

¹⁴ <http://www.gcsb.govt.nz/newsroom/reports-publications/Review%20of%20Compliance.pdf>

¹⁵ http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11206452

¹⁶ http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11112107

¹⁷ <http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/>

3.1.4. NZ participation in the global surveillance apparatus

As a part of the Five Eyes intelligence sharing network, New Zealand is complicit in the global mass surveillance of electronic communications conducted by the intelligence services in its partner countries, in particular the NSA and the UK's Government Communications Headquarters (GCHQ). New Zealand's participation in surveillance activities violates the human rights of non-New Zealand citizens.¹⁸

3.1.5. Metadata is personal

The Prime Minister has asserted that the GCSB does not “collect wholesale metadata about ordinary New Zealanders”, but has been unable to deny there is collection of New Zealanders' metadata by the NSA.¹⁹ While authorities worldwide have attempted to downplay the invasion of privacy represented by the collection of the metadata of a person's communications, new research has demonstrated it is extremely revealing of personal information. A recent study conducted by Stanford University found phone metadata was able to reveal details about the caller's personal details, such as medical conditions, religious affiliations, and financial status.²⁰

3.1.6. Mass surveillance is ineffective

Not only is mass surveillance of communications arbitrary and disproportionate, it is ineffective for its intended purpose and does not contribute to the safety of the public. Justifications for mass surveillance and the collection of metadata have continuously been cloaked in the language of “national security”. This justification has been debunked by several bodies²¹, including a US Government advisory panel, which concluded that a mass surveillance programme had not identified “a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation”.²²

3.1.7. Impact on innovation and jobs

18

<http://nzhumanrightsblog.com/newzealand/influential-european-parliament-committee-slams-new-zealand-for-being-part-of-nsa-mass-surveillance/#more-622>

19 http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11165930

20 <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>

21 http://www.newamerica.net/publications/policy/do_nsas_bulk_surveillance_programs_stop_terrorists

22

<http://www.pclob.gov/All%20Documents/Report%20on%20the%20Telephone%20Records%20Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf>

There is a huge economic cost attributed to maintaining communications surveillance infrastructure. The cost of interception capability under the TICS Bill (2013) has to be met by ICT providers.²³ Concerns have been raised by experts that this cost may bankrupt small businesses, raise user costs, and stymie innovation in the ICT sector. Moreover, users will look offshore for ICT services that ensure adequate protection of their data from prying eyes of the Government. Not only does this represent a backwards attitude to the rights of businesses and individuals, it also poses a missed opportunity in the post-Snowden era to attract privacy-conscious business and innovation to New Zealand.²⁴

3.2. Inadequate protection of rights

3.2.1. Bill of Rights Act is weak and ineffective

While the New Zealand Bill of Rights Act (1990) sets out the fundamental rights and freedoms of New Zealanders, it remains ineffective in preventing violations of rights because it lacks supremacy in relation to other legislation. Reports by the Attorney General on a bill violating the Bill of Rights have not provided deterrence. As it stands, the Bill of Rights Act can be trumped by a parliamentary majority, rendering it practically powerless.²⁵ This, for example, allowed for the passing of the GCSB Bill (2013), despite clear conflicts with rights of freedom of expression and freedom from search and seizure stipulated in the Bill of Rights Act.²⁶

3.3. Internet freedom

3.3.1. Assessment of New Zealanders' Internet freedom

A study by Joy Liddicoat of APC looked at New Zealanders' Internet freedom to assess how they experience and perceive their human rights when using the Internet.²⁷ It used the framework developed by United Nations' Special Rapporteur Frank La Rue on the promotion and protection of the right to freedom of opinion and expression.²⁸ Areas analysed included: Internet filtering and content blocking; website takedowns; and Internet intermediary liability. New Zealand was found to be non-compliant with four of the 29 Internet freedom indicators in the La Rue Framework, including access to legal information, and transparency by the private sector on content removal. The results of a further 11 were found to be unclear, including laws on national security.

3.4. Privacy

²³ <http://legislation.govt.nz/bill/government/2013/0108/latest/whole.html>

²⁴ <http://www.nbr.co.nz/article/why-tics-bill-could-put-new-zealand-ict-companies-out-business-ck-144864>

²⁵

<http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/government-communications-security-bureau-and-related-legislation-amendment>

²⁶ <http://www.lawsociety.org.nz/lawtalk/lawtalk-archives/issue-823/expansion-of-gcsb-intelligence-gathering-intrusive>

²⁷ <https://www.apc.org/en/irhr/i-freedom-nz/about>

²⁸ http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

3.4.1. Privacy as a human right

Privacy is a fundamental human right enshrined in international human rights law, rendering the government morally and legally obligated to protect New Zealanders' right to privacy. Article 17 of the International Covenant of Civil and Political Rights (ICCPR), ratified by New Zealand in 1978, states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.²⁹

Similar protection of the individual's privacy is also enshrined in the Universal Declaration of Human Rights (1948).³⁰

In response to the threat posed to this fundamental human right by digital communications surveillance, the United Nations General Assembly has called on all member States to end activities that violate the right to privacy.³¹

3.4.2. Kiwis care about privacy

As technological advancements expand many people's freedoms - such as access to knowledge, work, and communication with people all over the world - it also poses unparalleled opportunities for violation of the right to privacy. A Roy Morgan poll released in 2013 showed 62 percent of New Zealanders are concerned about the invasion of privacy made possible by new technologies.³² A survey conducted by UMR in March 2012 showed overall concern about privacy in the last 10 years has risen to 67 percent (up from 47 percent in 2001).³³ Also, 82 percent of survey respondents were worried about the Government silently sharing their personal information.

4. EXAMPLES OF GLOBAL LEADERSHIP

²⁹ <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>

³⁰ <http://www.un.org/en/documents/udhr/>

³¹ <http://www.un.org/apps/new/story.asp?NewsID=46780&Cr=privacy&Cr1>

³² <http://www.roymorgan.com/findings/2068-cyber-security-concerns-201401230121>

³³ <http://www.privacy.org.nz/news-and-publications/surveys/privacy-survey-2/>

4.1. Against surveillance of digital communications

4.1.1. International Principles of the Application of Human Rights to Communications Surveillance

In response to recent revelations regarding the extent of global surveillance of online communication, privacy organisations and advocates worldwide have produced a set of principles that Governments must comply with in order to adhere to international human rights law in the digital age, including, but not limited to:³⁴

- legality
- legitimate aim
- necessity
- proportionality
- due process
- transparency
- safeguards against illegitimate access
- public oversight

The aim is for human rights to be the overarching framework within which justified communications surveillance takes place.

4.1.2. International Principles of the Application of Human Rights to Communications Surveillance

After publication of the NSA revelations, the Parliament of the European Union (EU) launched an inquiry into the impact of mass surveillance on EU citizens. The Civil Liberties Committee started work in September 2013, and a report was published on February 12 2014.³⁵ The EU Parliament then passed a resolution on March 12 2014 criticising the over-reaching surveillance practices of the US government, and recommending the EU immediately halt the Transatlantic Trade and Investment Partnership (TTIP) agreement with the United States “as long as blanket mass surveillance activities and the interception of communications in EU institutions and diplomatic representations are not fully stopped”.³⁶

4.1.3. ECJ ruling on EU Data Retention Program

The European Court of Justice (ECJ) was requested by courts in Austria and the High Court of Ireland to examine whether the EU’s Data Retention Directive, which requires Internet operators to store user data for up to two years, is consistent with the Charter of Fundamental Rights of the EU. The court declared the directive invalid, stating that it “entails a wide-ranging and particularly serious interference with the

³⁴ <https://necessaryandproportionate.org/text>

³⁵ <http://www.europarl.europa.eu/news/en/news-room/content/20140210IPR35501/html/NSA-snooping-MEPs-table-proposals-to-protect-EU-citizens%27-privacy>

³⁶ <http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38203/html/US-NSA-stop-mass-surveillance-now-or-face-consequences-MEPs-say>

fundamental rights to respect private life and to the protection of personal data, without that interference being limited to what is strictly necessary”.³⁷ As a result of the court’s ruling, opponents of the directive are able to legally challenge the directive on a national level.

4.2. Protecting rights

4.2.1. Canadian Charter of Rights and Freedoms

In 1960, Canada passed into legislation the Bill of Rights to protect the rights and freedoms of Canadians.³⁸ However, the Bill of Rights proved ineffective and susceptible to narrow interpretation. As a result of calls for better protections for human rights, a bill of rights was elevated to supreme law with the Charter of Rights and Freedoms that forms part of the Constitution Act (1982), requiring all legislation to adhere to it. If Parliament passes a law that infringes on rights stipulated in the Charter, it will almost certainly have to prove in court that the law is “reasonably justified in a free and democratic society”.³⁹ Courts are empowered to overturn legislation that violates the rights stipulated in the Charter on the grounds that it is unconstitutional.

4.2.2. The charter of human rights and principles for the Internet

In an effort to ensure that rules governing the Internet adhere to international human rights standards, a group of individuals and organisations came together to draft the Charter of Human Rights and Principles for the Internet.⁴⁰ The charter outlines the application of human rights obligations to the Internet, including the right to access the Internet, the right to net neutrality, and the right to privacy on the Internet.⁴¹

4.2.3. Brazil’s Marco Civil

Brazil is leading the way globally in digital rights by enshrining them in law. Brazil has signed into law⁴² Marco Civil da Internet⁴³, a major piece of legislation outlining Internet rights.⁴⁴ The rights protected in the Marco Civil include freedom of expression online, guaranteed net neutrality, and protection of personal data. The Marco Civil was the result of an open and collaborative process that spanned two years. The initial drafts were open to comments online by the public and were debated in meetings throughout the country.

4.2.4. Sir Tim Berners-Lee

³⁷ <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

³⁸ <http://laws-lois.justice.gc.ca/eng/acts/c-12.3/FullText.html>

³⁹ <http://faculty.marianopolis.edu/c.belanger/quebechistory/federal/parl.htm>

⁴⁰ http://internetrightsandprinciples.org/site/wp-content/uploads/2014/02/IRP_booklet_2nd-Edition14Nov2013.pdf

⁴¹ <http://internetrightsandprinciples.org/site/campaign/>

⁴² <http://www.cnet.com/news/brazil-lays-down-the-law-with-internet-bill-of-rights/>

⁴³ http://en.wikipedia.org/wiki/Marco_Civil_da_Internet

⁴⁴ <http://infojustice.org/archives/32527>

On March 11, 2014, Sir Tim Berners-Lee issued a worldwide statement calling for greater protections of privacy and digital rights from the prying eyes of governments. He wrote: “On the 25th birthday of the web, I ask you to join in — to help us imagine and build the future standards for the web, and to press for every country to develop a digital bill of rights to advance a free and open web for everyone.”⁴⁵

4.3. Internet freedom

4.3.1. The Icelandic Modern Media Initiative

Public uproar following the uncovering by Wikileaks of a court order banning a national broadcaster from reporting on a bank’s exposure to debt default led to legislative efforts to cement Iceland as a haven for data protection and Internet freedom. The Iceland Modern Media Initiative has involved a process of passing 13 laws covering, among others, the following areas:⁴⁶

- freedom of information
- whistle-blower protections
- source protection
- communications protection
- limiting prior restraint
- protection of Internet intermediaries

Enshrining these protections in law has placed Iceland at the fore of attracting Internet start-ups, media organisations, and data centres.⁴⁷

4.3.2. NETmundial

At the end of April 2014, Brazil hosted NETmundial, the Global Multi-stakeholder Meeting on the Future of Internet Governance.⁴⁸ The meeting focused on the future of Internet governance and a roadmap for its development. A WikiLeaks publication of the draft outcome document showed the emphasis was on human rights online, an open Internet, and mass surveillance.⁴⁹

5. POLICY PROPOSALS

5.1. Review surveillance laws

⁴⁵ <http://googleblog.blogspot.com/2014/03/on-25th-anniversary-of-web-lets-keep-it.html>

⁴⁶ <https://immi.is/index.php/projects/immi>

⁴⁷ <http://www.freedomhouse.org/report/freedom-net/2013/iceland>

⁴⁸ <http://netmundial.br/>

⁴⁹ <https://wikileaks.org/netmundial-outcome/>

Acknowledge and apologise for past violations: The Internet Party will immediately ensure that the 88 people illegally spied on by the GCSB are informed about the unlawful violation of their privacy and that they are issued an apology from the Government.

Review legislation governing the GCSB: The Internet Party will immediately repeal the GCSB Bill (2013) to remove the legal basis for mass surveillance in New Zealand. The party will initiate an end-to-end review of the GCSB Act (2003) and the respective roles played by other surveillance bodies. The review will take into account future requirements and interests of the country's national security, while ensuring that it conforms to New Zealand's international human rights obligations. An independent cross-party oversight committee, chaired by the Leader of the Opposition and including independent non-political experts, will be established within Parliament to effectively ensure that the security agencies are operating within their respective legislative frameworks.

Review intelligence co-operation agreements: As part of the fight against unjustified and mass surveillance and in favour of a strong, independent New Zealand, the Internet Party insists that New Zealand should immediately hold a review of all international intelligence co-operation agreements, with a view to leaving the Five Eyes intelligence sharing network and exercising sovereign control of New Zealand's intelligence agencies. All reviews of intelligence co-operation agreements must take into account the future interests of New Zealand rather than continue colonial arrangements.

Review telecommunications interception capability requirements: The Internet Party will immediately repeal the TICS Bill (2013). In consultation with the ICT industry, a new Bill will be put forward that provides a better balance between national security and human rights in the digital age. Costs and constraints imposed on the ICT industry will be a major consideration.

5.2. Strengthen human rights protection

Review Bill of Rights Act: The Internet Party will initiate a fast-tracked review of the Bill of Rights Act (1990) by the Law Commission to ensure it is fit for purpose in the digital age and is capable of safeguarding human rights in an environment of overarching digital communications surveillance by the State.

The Law Commission will also be asked to recommend if amendments to the Bill of Rights Act are sufficient or whether a new Bill of Digital Rights is required to enshrine Internet freedoms such as:

- right to access the Internet
- freedom from filtering and content blocking
- freedom from censorship
- right to private communications
- protection of communications metadata
- right to anonymity
- right to secure data
- liability for Internet intermediaries

Any new Bill of Digital Rights will be developed through an inclusive and open public process, allowing citizens to co-develop the bill through an online platform and witness the bill evolving to reflect the will of the public.

Elevate Bill of Rights: Following a review of the Bill of Rights Act, the Internet Party will propose that the Bill of Rights be elevated to superior legislation so that all future legislation must comply with its provisions. It will also change the Bill of Rights Act to be entrenched legislation. This means a future government could only change it under special circumstances, for example by holding a referendum or by a majority of at least 75% in Parliament.

5.3. Strengthen Internet freedom

Legislate website takedowns and role of Internet intermediaries: The Internet Party will introduce new legislation to require due process before websites are taken down, with adequate checks and balances. A general safe harbour for Internet intermediaries will be provided to conditionally shield them from liability for users' actions. The legislation will clarify the responsibilities and liabilities of Internet intermediaries for safeguarding human rights online. In addition, the Internet Party will introduce a principles-based approach to making laws for the digital age that works in harmony with the Internet and its widespread effect on society.

Regulate Internet filtering: The Internet Party will introduce new legislation to provide authorisation, oversight, and limitation of scope for voluntary Internet filtering of child exploitation material. Any change in scope of Internet filtering will require Parliament's approval. Annual reporting of the filter's efficacy will be required.

Transparency reporting: The Internet Party will require all Internet intermediaries operating in New Zealand to issue a half yearly Transparency Report that details requests they have received, and actions taken in response to requests for taking down online content and actions involving human rights. Publication of Internet filtering policy will also be mandatory.

In addition, the Government will be required to publish an Annual Transparency Report. The Government will be required to issue a public undertaking that no requests or orders to the ICT industry for interception capability (except the details of individual interception orders) will be made in secret. Summary information and the nature of interception capability required from the ICT industry - but not such details that may compromise national security - will be published each year.

An open and free Internet: The Internet Party will require the New Zealand Government to take a more proactive approach to international discussions and initiatives about the future of Internet governance. Support will be provided for international technical moves to strengthen the security and fabric of the Internet. A multi-stakeholder approach to developing public policy for the Internet and a single, global Internet will be advocated. New Zealand will participate in the transition of US responsibilities in the global Internet Domain Name System to the "global multi-stakeholder community".



5.4. Implement Privacy Act reform

The Internet Party will review outstanding recommendations from the Law Commission's review of the Privacy Act and fast track legislative changes to implement the accepted recommendations.