GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

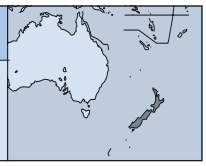
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

NEW ZEALAND

Eyes on New Zealand



Association for Progressive Communications (APC) and Tech Liberty
Joy Liddicoat and Tech Liberty[1]
www.apc.org, www.techliberty.org.nz

Introduction

New Zealand is a small country, with a population of less than five million, situated in the far reaches of the southern hemisphere. But its physical remoteness belies a critical role in the powerful international intelligence alliance known as the "Five Eyes",[2] which has been at the heart of global controversy about mass surveillance. This report outlines the remarkable story of how an international police raid for alleged copyright infringement activities ultimately became a story of illegal spying on New Zealanders, and political deals on revised surveillance laws, while precipitating proposals for a Digital Rights and Freedoms Bill and resulting in the creation of a new political party. We outline how civil society has tried to respond, and suggest action points for the future, bearing in mind that this incredible story is not yet over.

Background: New Zealand's role in the Five Eyes

The impact of the revelations of mass surveillance and New Zealand's role must be seen against the backdrop of the country's role in the Five Eyes alliance. Nicky Hager, New Zealand's most prominent investigative journalist, says "for the most part [New Zealand's role in the Five Eyes] was an accident of history."[3] Arising from intelligence-sharing agreements among five countries during and after World War II, the main agency responsible for its day-to-day operations in New Zealand is the Government Communications Security Bureau (GCSB).[4]

A key aspect of this intelligence-sharing regime is a legal framework that provides differing levels of protections for internal (national) versus external (extraterritorial) communications, or those relating to national citizens versus non-nationals. This framework discriminates on grounds of national origin, and in doing so purports to step around human rights protections from interferences with the right to privacy of communications by the governments of the Five Eyes, claiming that such protections apply only to nationals or those within their territorial jurisdiction.[5]

Historically, the main purpose of the GCSB under this legal framework has been to spy on our neighbours in Asia and the South Pacific on behalf of the Five Eyes. This enabled the GCSB to claim that it did not spy on New Zealand citizens or permanent residents. Public assurances to this effect were given on a number of occasions by both the GCSB and the New Zealand government.[6]

Case study: Mega Upload – the move to domestic surveillance

In 2012 the New Zealand Police assisted the United States of America's Federal Bureau of Intelligence (FBI) to carry out a raid on the house of Mr Kim Dotcom, founder of Mega Upload, an online file-sharing platform. Mr Dotcom had migrated to New Zealand from Hong Kong and was living in New Zealand legally as a permanent resident. The extraordinary raid of the house (replete with a helicopter bringing armed police officers into the house grounds to seize computers and other property), the seizure of the Mega Upload online service, and Mr Dotcom's subsequent arrest and criminal prosecution, received huge media attention both in New Zealand and overseas.[7]

Mr Dotcom is an enigmatic figure, who has maintained a vigorous defence of all charges and high and consistent media presence through public en-

1 TechLiberty is a New Zealand group advocating for civil liberties online: www.techliberty.org.nz

2 The "Five Eyes" countries are New Zealand, Australia, Canada, the United Kingdom and the United States of America. The alliance operates an integrated global surveillance arrangement that covers the majority of the worlds' communications. For an overview of legal arrangements see: APC et al. (2014). Joint Submission in Connection with General Assembly Resolution 67/167, "The right to privacy in the digital age". https://www.apc.org/en/pubs/submission-office-high-commissioner-human-rights-r

3 Hager, N. (1996). *Secret power: New Zealand's Role in the International Spy Network*. Port Nelson: Craig Potton Publishing, p. 58.

4 The first law authorising its operations was in 1977, followed by the Government Communications Security Bureau Act 2003.

5 APC et al. (2014). Op. cit., Appendix 1.

6 See also Hager, N. (2013, April 10). Who is really responsible for the GCSB shennanigans? *Pundit*. www.pundit.co.nz/content/who-is-really-responsible-for-the-gcsb-shenanigans

7 For an overview of the case, see: https://en.wikipedia.org/wiki/Megaupload_legal_case

gagement against leading politicians, including the prime minister. There are many factors to the case which remain outstanding – extradition issues, validity of search warrants, and many other legal matters outside the scope of this report. However, in relation to surveillance issues, the case against Mr Dotcom revealed that the GCSB had been spying on him and sharing information from its activities with New Zealand law enforcement officers who were also dealing with the FBI in the investigation of Mega Upload. Public outrage followed the discovery that the GCSB were in fact spying on New Zealanders and resulted in the prime minister establishing an independent investigation by Rebecca Kitteridge.

The Kitteridge Report[8] revealed that the GCSB activity was not an isolated case: in fact 88 unnamed New Zealanders had been spied on over many years.[9] The report concluded that the GCSB based their operations on a faulty interpretation of the relevant New Zealand law (for example, they believed the prohibition on spying did not apply where there was a warrant and did not apply to "metadata" because metadata was not a "communication"), and that the law was unclear and therefore the GCSB were not at fault.[10] Various recommendations were made for changing GCSB operations and law.

Prime Minister John Key immediately responded that the report made "sobering reading" and further: "I am embarrassed to say that I heard the unequivocal assurances and read the clear prohibition in the GCSB legislation, and I believed that they did not spy on New Zealanders. But it turns out they have been regularly spying on New Zealanders from before 2003 and since. They have seriously let down the public."[11] Signalling a need for law reform, the prime minister also said: "In addition, the Act governing the GCSB is not fit for purpose and probably never has been."[12]

The Kitteridge Report had been leaked, much to the fury of government ministers, and a parliamentary inquiry was launched. The prime suspect was Peter Dunne, a parliamentarian holding a single vote supporting the coalition government. Data about both Dunne's movements and those of journalists in the parliamentary precinct (from security card swipe records at various doors in different buildings) were handed to the investigation. Dunne and journalist Andrea Vance's private phone records and emails from a three-month period were also provided to the investigation, without their knowledge or consent. These actions were widely seen as an attack on privacy and press freedom, sparking intense commentary from local journalists and media outlets. Dunne denied he was the source of the leak and asserted his rights to privacy,[13] but was forced to resign his ministerial portfolio.[14]

Throughout this time, the Snowden revelations also kept coming, contributing to ongoing media focus and providing a wider global backdrop to the GCSB scandal and the proposed law reforms.

It was in this context that two new laws were introduced. The first, the GCSB Bill, was designed to restructure the GCSB and establish its legal basis more clearly. But the new laws went much further, retrospectively validating the GCSB action and fundamentally shifting the permitted surveillance activities to include surveillance of New Zealand citizens. Rather than clarifying that the GCSB could not spy on New Zealanders, the new law simply extended the authority to do so and validated the previously unlawful activity, clearly violating privacy rights. There was widespread consternation and opposition from legal groups, the technical community, business, human rights organisations and community organisations. The New Zealand human rights commission also took the unusual step of preparing a separate report for the prime minister highlighting serious concerns with the proposals.

The second law, the Telecommunications Interception Capability and Security Act (TICS), gave sweeping new powers to the GCSB, making new network security measures by all network operators including telecommunications companies, such as submission of security measures to the newly constituted GCSB. Thomas Beagle from Tech Liberty noted:

> The [TICS] bill codifies the government's assertion that all digital communications (which is increasingly becoming equivalent to "all communications") must be accessible by government agencies. The limits imposed are minimal and laws such as the GCSB Act override any limits included in TICS. Furthermore, to ensure that the government can do this, the GCSB will now have oversight of the design and operation of New Zealand's communications networks. They will be able to veto any decision made by the network

8 Kitteridge, R. (2013). *Review of Compliance at the GCSB.* www.gcsb.govt.nz/news/publications

9 Ibid.

10 Bennett, A. (2013, April 9). CSB report: 88 cases of possible illegal spying uncovered. *New Zealand Herald*. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10876424

11 Key, J. (2013, April 9). PM releases report into GCSB compliance. *Beehive.govt.nz*. www.beehive.govt.nz/release/pm-releases-report-gcsb-compliance

12 Ibid.

13 Shuttleworth, K. (2013, July 30). Reports phone records released. *New Zealand Herald*. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10905495

14 Burr, L. (2013, June 7). Peter Dunne resigns as minister. *3 News*. www.3news.co.nz/Peter-Dunne-resigns-as-minister/tabid/1607/articleID/300658/Default.aspx

operators that might impact on security or, more likely, limit their ability to spy as they see fit.[15]

Under the TICS, the GCSB now has the ability to approve or refuse to approve all significant changes to New Zealand's telecommunications infrastructure. This new power far exceeds any role of the GCSB in the Five Eyes, extending its oversight to business and other private sector activities.

At the same time as these two new laws were being passed, a new internet censorship law aimed at harmful online speech, the Harmful Digital Communications Bill, was also before parliament.[16] The local internet community worked hard to respond to these new measures, including bringing national attention to concerns about the role of New Zealand in the Five Eyes, highlighting human rights concerns and the need for limitations on human rights only in exceptional and narrow circumstances, in line with the 13 International Principles on the Application of Human Rights to Communications Surveillance.[17]

The degree of public interest was enormous. Large public meetings and street rallies were held throughout the country, fuelled by the Snowden revelations and leaks of information about the role of New Zealand in the Five Eyes. Thousands of people rallied, started and joined online campaigns, with both online and offline media and journalists engaging.

Overall, it was an intense period of constant media coverage and political focus. At times developments happened daily, even hourly, making it difficult to maintain an overview of what was happening, how developments were related and to think strategically about how to respond. Views were also divided: some thought privacy issues were not relevant in an internet age; others considered it was legitimate for the government to carry out surveillance. Despite widespread public opposition to the GCSB Bill, the prime minister went so far as to claim that New Zealanders cared more about how many fish they were allowed to catch than they did about their online privacy.[18]

By the end of 2013 both the GCSB and TICS Bills were law and campaigns to counter them had proved ineffective. But the awareness of internet-related policy issues had grown enormously. In March 2014 the main political opposition, the Labour Party, announced plans for a new Digital Bill of Rights.[19] Within weeks Gareth Hughes, a Greens political party member of parliament, launched a new Digital Rights and Freedoms Bill,[20] drawing heavily on the global civil society Charter of Internet Rights and Principles,[21] with protections for encryption, privacy and freedom from search, surveillance and interception of communications.

Implications

The GCSB and TICS laws were passed, while New Zealand continues to affirm its security stance with the United Kingdom[22] and the Five Eyes alliance. Yet the political and legal fallout from the Kim Dotcom raid has extended far beyond anything that could ever possibly have been imagined.

What began as mutual assistance in law enforcement for alleged intellectual property rights violations (which sparked the original police raid and seizure of Mega Upload) has ended in multiple investigations, revelations of spying, new laws, and a sea change in regulation affecting the internet in New Zealand. We have even seen the birth of a new political party, the Internet Party, founded by Mr Dotcom, which has formed an alliance with the Mana Party and is contesting the general election in September 2014.[23]

But the pace of regulatory intervention, its technical aspects, and the intensely political nature of the proposals make it very difficult for many New Zealanders to engage meaningfully. More major law reforms were announced in May 2014, with a wholesale review of the Privacy Act which will include new measures for data sharing by government agencies, mandatory reporting of data breaches, and a new offence of impersonation.

While this review is welcome, and there is a good Privacy Commissioner[24] who has knowledge of internet-related issues, the policy review will also require close scrutiny and engagement from civil society groups. Legal academics are still only beginning to focus on surveillance and privacy[25]

15 Tech Liberty. (2013 November 5). TICS - Second spy law passes. *Tech Liberty*. techliberty.org.nz/tag/gcsb

16 The Harmful Digital Communications Bill 2012 deals with harmful online content and has been reported back from Select Committee. It is not expected to become law until 2015. See also Paton, L. and Liddicoat, J. (2013). New Zealand. In APC and Hivos, *Global Information Society Watch 2013: Women's rights, gender and ICTs*. www.giswatch.org/en/country-report/womens-rights-gender/new-zealand

17 www.necessaryandproportionate.org

18 John Key, press conference, 12 August 2013. www.3news.co.nz/Key-NZers-care-more-about-snapper-than-GCSB/tabid/817/articleID/308665/Default.aspx

19 Cunliffe, D. (2014, March 9). Digital Bill of Rights. *Labour*. https://www.labour.org.nz/media/digital-bill-rights

20 internetrightsbill.org.nz/ten-internet-rights-and-freedoms

21 internetrightsandprinciples.org/site/

22 McCully, M. (2013, January 13). NZ-UK joint statement on cyber security. *Beehive.govt.nz*. www.beehive.govt.nz/release/nz-uk-joint-statement-cyber-security

23 Bennett, A. (2014, May 27). Mana confirms election year deal with Internet Party. *New Zealand Herald*. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11262597

24 Privacy Commissioner John Edwards: privacy.org.nz

25 For example, the University of Otago held a symposium on Surveillance, Copyright and Privacy in January 2014: https://blogs.otago.ac.nz/scpconf/programme-of-events/abstracts-of-talks

and in general the legal community has been slow to grasp the human rights implications of internet-related policy and regulatory measures.

In some cases rights-affirming changes have been made to draft laws,[26] but change is often difficult once laws are drafted because of political issues. In the case of the GCSB Bill, for example, it quickly became apparent that the government was unlikely to make major changes. Dunne, the politician who had refused to disclose his own communications to parliamentary investigators, ultimately voted for the GCSB Bill in a political deal widely condemned as a cynical "trade off for privacy".[27] His ministerial portfolio was later reinstated.[28]

In addition, the Kitteridge Report had found that the legal authority for collection of metadata was unclear and that it should be clarified. However, the government declined to do so in the GCSB and TICS laws and instead went further, extending the powers of the GCSB and the legal regime for spying on New Zealanders.

The 13 Principles are being used to support advocacy and were referenced in submissions on the Harmful Digital Communications Bill.[29] But while these have been helpful for civil society, it is difficult to see if these have had lasting impact in a country whose government's foreign policy is so closely aligned to the Five Eyes alliance. One encouraging sign is that the Principles have been cited in the Internet Party's policy on privacy and internet freedom.[30]

New Zealand prides itself on its human rights reputation. But the reality is that our human rights online are more at risk. The result from these events is that threats to internet freedom have actually increased: instead of curtailing the GCSB's powers, new laws provide much stronger, direct state-sanctioned surveillance (including the use of metadata) by the GCSB, which it can use in domestic law enforcement. In the public mind, significant issues of trust remain, but it is unclear how this might affect the 2014 national elections.

New civil society voices have emerged in the last two years, but these groups need more support because the volume, speed and size of internet-related policy is growing rapidly. In this environment, which is also highly politically charged, it is vital to have strong independent voices, and groups such as Tech Liberty are being increasingly called on to respond and help to inform public understanding and debate.

In a further development, in July 2014, the United Nations High Commissioner for Human Rights issued a damning report on issues of mass surveillance. The report concluded that the collection of metadata is a violation of the right to privacy and human rights obligations apply without discrimination.[31] It is unfortunate that the report was not available during the Kitteridge inquiry, which concluded that the legality of metadata collection was unclear. But the clear and unequivocal UN report now needs to be followed up and actioned in New Zealand. Regular monitoring of New Zealand internet freedom is also needed so that it can be available quickly to support advocacy when needed.[32]

Action steps

Tech Liberty is one of only a handful of New Zealand civil society groups and individuals working on internet-related human rights issues, including privacy and surveillance. Others include the New Zealand Council for Civil Liberties, New Zealand Law Society, and InternetNZ. As a voluntary group with limited resources, the task of monitoring and advocating is often difficult. More support and resources are needed if the network of voices that has the capacity to engage in these important debates and activities is to be grown and strengthened. This includes the legal and academic communities.

Specific actions that need to be taken include:

- Support civil society advocacy efforts, including capacity building for those groups for whom internet-related human rights issues are still new.
- Regularly update the NZ internet freedom index[33] to enable periodic monitoring of threats to internet freedom, and use these results in reporting on New Zealand's human rights performance.
- Review, and where necessary amend, the GCSB and TICS Acts in light of the United Nations High Commissioner for Human Rights report which finds, among other things, that collection of metadata is a violation of the right to privacy.
- Bring the New Zealand experience to the United Nations Human Rights Council session on the right to privacy in the digital age in September 2014.

26 Tech Liberty. (2014, May 27). HDC Bill reported back by Select Committee. *Tech Liberty.* techliberty.org.nz/hdc-bill-reported-back-by-the-select-committee

27 National Business Review. (2014, August 14). Swing vote Dunne supports GCSB Bill after changing tune on domestic spying. *National Business Review*. www.nbr.co.nz/article/swing-vote-dunne-supports-gcsb-bill-after-changing-tune-domestic-spying-peters-holds-out-ck-

28 AAP. (2014, January 21). Leak forgotten, Dunne back as minister. *MSN.nz*. news.msn.co.nz/nationalnews/8787062/dunne-reinstated-as-minister

29 For example, by Tech Liberty: techliberty.org.nz/submission-harmful-digital-communications-bill/#more-1968

30 Internet Party, Privacy and Internet Freedom Policy, Clause 4.1.1. https://internet.org.nz

31 See also Association for Progressive Communications. (2014, July). Op. cit.

32 https://www.apc.org/en/irhr/i-freedom-nz/about

33 freedomindex.apc.org/index.php/Main_Page