PRIVACY INTERNATIONAL

Human Rights Committee 116th Session

The Right to Privacy in New Zealand

Privacy International's submission in advance of the consideration of the periodic report of New Zealand, Human Rights Committee

116th Session, March 2016

1. Introduction

Privacy International notes New Zealand's written replies to the list of issues prior to reporting in relation to the New Zealand's laws, policies and practices related to interception of personal communications.

A review of the security and intelligence legislation is currently underway in accordance with the Intelligence and Security Committee Act. It is expected that the Parliament will consider the review in 2016. Hence this represents a significant opportunity to amend the current legislation regulating the powers of intelligence agencies to bring into line with article 17 of the International Covenant on Civil and Political Rights.

2. Interception of communications by intelligence agencies

Government Communications Security Bureau (GCSB)

The Government Communications Security Bureau (GCSB) is the main signal intelligence agency in New Zealand. Under the Government Communications Security Bureau Act (amended in 2013, hereinafter GCSB Act), its functions are related to cyber security, foreign intelligence gathering and providing assistance to the New Zealand Police, Defence Forces and Security Intelligence Service.[1]

Section 8D of the GCSB Act requires that the GCSB performs its functions "in accordance with New Zealand law and all human rights standards recognised by New Zealand law, except to the extent that they are, in relation to national security, modified by an enactment". The NZ Bill of Rights Act 1990 (BORA) protects against unreasonable search and seizure (Section 21); and the reference to "human rights standards" should be interpreted to include the International Covenant on Civil and Political Rights.[2]

The Act provides the GCSB with powers to intercept communications and accessing communications infrastructures when performing its function of cyber security and foreign intelligence gathering (section 13).

The Act prohibits the interception of private communications of New Zealand citizen or permanent resident when the agency acts for the purpose of gathering foreign intelligence (section 14).

Under section 5 of BORA, rights and freedoms must "be subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society." The New Zealand courts have adopted a necessity and proportionality test to assess measures limiting human rights.[3] However, the GCSB Act contains no such limitations. Section 4 of BORA makes clear that provisions in New Zealand laws cannot be revoked by courts by reasons that

1 See Section 8 of the Act, available here: http://www.legislation.govt.nz/act/public/2003/0009/latest/DLM187178.html?src=qs
2 See http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html
3 See the NZ Supreme Court judgment of Tipping J in Hansen v R [2007] NZSC 7, paragraph 104, available here: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj_pL3o2ufKAhVC7xQKHR9jApsQFgggMAA&url=https%3A%2F%2Fwww.courtsofnz.govt.nz%2Fcases%2Fpaul-rodney-hansen-v-the-queen%2Fat_download%2FfileDecision&usg=AFQjCNEGd5P8oMQy5nZltMcackPu1n9bxw&sig2=2h7v3ZEmeG-oqgvb6KgeMg&cad=rja

they are inconsistent with BORA. Hence the New Zealand courts can only use BORA principles as an interpretative tool to the provisions of the GCSB Act. Interception of communications can relate to "classes of persons" or "classes of places", which is too broad to allow a proper determination of necessity and proportionality (Section 15A).

Further the conditions for interception of personal communications are not strictly limited to what is necessary and proportionate for the achievement of a legitimate aim, as required under human rights law. Instead, the conditions that these requests for warrants must fulfil are worded in broad language, such as "outcome is not likely to be achieved by other means" and "satisfactory arrangements" are in place (Section 15A).

There is no judicial prior authorisation for interception of communications or access to communications infrastructures. Instead the relevant warrant is authorised by the Minister. The Commissioner of Security Warrants, a retired judge, is only required to jointly authorise interception warrants when the communications of New Zealanders may be intercepted.

The warrant regime described above under the GCSB Act does not apply to the activities the GCSB carries out in order to provide assistance and support to the New Zealand Police, Defence Forces and Security Intelligence Service. Concerns about the scope of the GCSB's interception of communications outside New Zealand has emerged following the release of NSA documents last year. In its oversight role of the activities of the intelligence services, New Zealand's Inspector-General of Intelligence and Security announced an investigation on the reports of the GCSB's communications surveillance in the South Pacific, including alleged interception of communications of New Zealanders. Her investigation commenced in May 2015. The investigation is on going.[4]

New Zealand Intelligence Service

As noted in the government report, beyond the GCSB Act the only other laws that provides authority to intercept communications are the Search and Surveillance Act 2012 and the New Zealand Security Intelligence Service Act (NZSIS Act.)

Under the NZSIS Act[5] , the Security Intelligence Service has, inter alia, the function to "obtain, correlate, and evaluate intelligence relevant to security" (Section 4(1)(a)). The process for authorising intelligence warrants (interception, seizure of communications or electronic tracking) distinguish between domestic and foreign warrants.

Similarly to the provisions under the GCSB Act, a domestic intelligence warrant is issued jointly by the Minister and the Commissioner of Security, whereas a foreign intelligence warrant is issued by the Minister alone, who must be satisfied that there are reasonable grounds for believing that the subject of the

4 See Inspector-General annual report 2015, available here: http://www.igis.govt.nz/assets/IGIS-Annual-Report-2015.pdf
5 Available here: http://www.legislation.govt.nz/act/public/1969/0024/latest/versions.aspx

intelligence warrant is not a New Zealand citizen or permanent resident and that any places specified are occupied by a foreign organisation or a foreign person. An intelligence warrant provides an authorisation for the Service to intercept or seize any communication, document, or thing not otherwise lawfully obtainable or to undertake electronic tracking of identified persons.

Before the Minister (and the Commissioner for domestic warrants) issue an intelligence warrant they must be satisfied on the basis of the evidence provided on oath by the Director of the Service that: the warrant is necessary for the detection of activities prejudicial to security or that it is necessary for the purpose of gathering foreign intelligence information that is essential to security; the value of the information sought to be obtained under the proposed warrant justifies the particular interception or seizure or electronic tracking; the information is not likely to be obtained by any other means; and any communication sought to be intercepted or seized under the proposed intelligence warrant is not protected by lawyer/client confidentiality. (Section 4A)

The lack of judicial authorisation for the interception of communications of non New Zealanders in both the GCSB and the NZSIS Acts raise serious human rights concerns. The UN High Commissioner for Human Rights and the UN Special Rapporteur on counter-terrorism and human rights have noted how several legal regimes on interception of personal communications, like in New Zealand, distinguish between obligations owed to nationals and non-nationals and residents and non-residents, providing external communications with lower or non-existent protection, in ways that are discriminatory and incompatible with Article 26 of the ICCPR.[6] The UN Special Rapporteur on counter-terrorism concluded that states "are legally bound to afford the same protection to nationals and non-nationals, and to those within and outside their jurisdiction".[7] Similarly the Human Rights Committee has consistently recommended that any interference with the right to privacy in the context of communications surveillance complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance.[8]

3. Metadata

Privacy International is concerned about the uncertainty as to whether the New Zealand legislation on interception of communications regulate the collection and analysis of metadata.

Under the Telecommunications Interception Capability and Security Act 2013 (TICSA), "call associated data" is among the type of information that

6 See report of the UN High Commissioner on Human Rights on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014; and report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014. During the debate on the GCSB Bill, the NZ government justified the differential treatment between New Zealanders and foreigners, including on the grounds that "distinction reflects the greater expectation of privacy of citizens and permanent residents in respect of intelligence gathering and is also consistent with the lesser expectation of privacy, if any, in information held outside New Zealand and/or foreign intelligence information." (Full report available here: http://www.justice.govt.nz/policy/constitutional-law-and-human-rights/human-rights/bill-of-rights/government-communications-security-bureau-and-related-legislation-amendment)

7 Report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, paragraph 43.

8 See, for example, Human Rights Committee, concluding observations on the United Kingdom, July 2015.

telecommunications network or services must be able to provide the relevant New Zealand surveillance agencies. TICSA defines call associated data quite broadly as to include, but not be limited to, "(i) the number from which the telecommunication originates; (ii) the number to which the telecommunication is sent; (iii) if the telecommunication is diverted from one number to another number, those numbers; (iv) the time at which the telecommunication is sent; (v) the duration of the telecommunication; (vi) if the telecommunication is generated from a mobile telephone, the point at which the telecommunication first enters a network" (Definitions).

As noted in the government report, TICSA itself does not provide agencies with interception powers. However the legislation that regulates such interception does not define call associated data. The GCSB Act, for example, defines communication quite broadly, but it is not clear whether it intended to cover metadata. In 2013, the NZ Prime Minister declared that the provisions in the GCSB Act cover metatada.[9] However, the lack of clarity is of concern, particularly in light of the observations made in the review of the GCSB in 2013 (Kitteridge report), which found that the legal authority for collection of metadata was unclear and required further clarification.[10]

The interception, collection and use of metadata interfere with the right to privacy, as it has been recognized by human rights experts, including the UN Special Rapporteur on freedom of expression, the UN Special Rapporteur on counter-terrorism and human rights and the High Commissioner for Human Rights.[11] The Court of Justice of the European Union noted that metadata may allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained" and concluded that the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[12]

4. Interception of satellite communications

According to NSA documents released in 2015, New Zealand's GCSB carries out "full take" interception of satellite communications from the Waihopai satellite communications interception station.[13] This is reportedly part of a Five Eyes network of satellite communication sites around the world allowing the interception of communications from multiple satellites.[14]

9 "There have been claims this Bill [the 2013 amendments to the GCSB Act] offers no protection of metadata and allows for wholesale collection of metadata without a warrant. None of that is true. Metadata is treated the same in this Bill as the content of a communication. So when the GCSB wants to access metadata, it is treated with the same level of seriousness and protection as if the GCSB was accessing the actual content of a communication." Available at: http://www.stuff.co.nz/national/politics/9070452/GCSB-Prime-Minister-John-Keys-speech

10 In the Kitteridge report the GCSB revealed that they believe that "metadata was not a communication" and that they "could, on request, lawfully obtain and provide information about metadata involving New Zealanders, without the authority of a warrant". Review of compliance at the Government Communications Security Bureau, March 2013, available at: http://www.gcsb.govt.nz/assets/GCSB-Compliance-Review/Review-of-Compliance.pdf

11 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

12 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

13 See http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11411759

14 For an overview and an explanation of the technical capabilities, see Desmond Ball, Duncan Campbell, Bill Robinson and Richard Tanter, Expanded Communications Satellite Surveillance and Intelligence Activities utilising Multi-beam Antenna Systems, The Nautilus Institute for Security and Sustainability, 2015

The potential of mass, indiscriminate interception of personal communications by capturing and storing satellite communications raises serious concerns on the right to privacy. Further, the GCSB Act contains no explicit regulation of the interception of satellite communications. Instead, it seems that certain forms of satellite communication interceptions might be covered under Section 16 of the Act, which are at the discretion of the Director of the GCSB and requires no warrants.[15]

5. Intelligence sharing

Under the GCSB Act and the NZSIS Act, the GCSB and the New Zealand Intelligence Services can cooperate not only with other domestic agencies, but also with foreign agencies. Privacy International is concerned that the acts do not specify the procedures and limits of such cooperation. Particularly, when it comes to sharing of data, that under the GCSB Act and the NZSIS Act the directors enjoy wide discretion to share intelligence obtained under these acts, including to foreign intelligence agencies.

Under Section 25 of the GCSB Act, the Director of GCSB may communicate the "incidentally obtained intelligence" to 'any other person [public authority in New Zealan or abroad] that the Director thinks fit to receive the information' for purposes such as "preventing or detecting serious crime in New Zealand or any other country" and "identifying, preventing, or responding to threats or potential threats to the national security of New Zealand or any other country." Similarly, Section 4H of NZSIS Act allows the Director of the Security Services to retain and share information for the purpose of preventing or detecting serious crimes (defined for offences punishable by two or more years' imprisonment). It suggests that it is a the discretion of the Director to decide to whom to share such information (which could include sharing it with foreign intelligence agencies.)

The decision of the Directors to share such intelligence is not subject to judicial or even ministerial warrants. Concerns about this broad, unfettered powers were raised by a number of organisations when the GCSB bill was debated.[16]

The lack of specific regulations on information sharing is of particular concern in light of the revelations of the direct access to intelligence databases of the members of the five eyes alliance, including New Zealand.[17]

6. Recommendations

Based on the above observations, Privacy International suggests the following recommendations for the New Zealand government:

- Take all necessary measures to ensure that its surveillance activities,

15 On Section 16 authorisations, see annual report of the Inspector-general, available here: http://www.igis.govt.nz/assets/IGIS-Annual-Report-2015.pdf

16 See in particular, submission of the New Zealand Law Society, available at: https://www.lawsociety.org.nz/__data/assets/pdf_file/0007/68389/Government-Communications-Security-Bureau-and-Related-Legislation-Amendment-Bill-140613.pdf ; submission of the New Zealand Council of Trade Unions Te Kauae Kaimahi, available at: http://union.org.nz/sites/union.org.nz/files/GCSB%20Bill%20CTU%20submission%20June%202013.pdf; and submission by the Human Rights Foundation of New Zealand, available at: https://humanrightsfoundation.wordpress.com/2013/07/03/gcsb-bill-out/

17 See https://theintercept.com/2014/09/15/snowden-new-zealand-surveillance/

both within and outside the New Zealand, conform to its obligations under the Covenant, including article 17; in particular, measures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under surveillance, which includes refraining from engaging in mass surveillance;

- In particular reform the GCSB Act and the NZSIS Act in order to ensure that (i) any interception of communications, including of metadata, is authorised by a judicial authority and it is necessary and proportionate to the achievement of a legitimate aim; (ii) the laws are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit on the duration of surveillance, and procedures for the use and storage of data collected; (iii) the conditions for retaining and sharing collected information are strictly defined and subject to independent review; (iv) the interception and use of satellite communications is likewise regulated and subject to judicial authorisation;

- Review the practice of intelligence sharing with foreign agencies to ensure its compliance with the right to privacy, under Article 17 of the Covenant.