PRIVACY INTERNATIONAL

Stakeholder report
Universal Periodic Review
32nd session period – New Zealand

The Right to Privacy in New Zealand

Submitted by Privacy International

July 2018

The Right to Privacy in New Zealand

July 2018

PRIVACY INTERNATIONAL

www.privacyinternational.org

INTRODUCTION

1. This Universal Periodic Review stakeholder report is a submission by Privacy International.[1] Privacy International is a human rights organisation that works to advance and promote the right to privacy around the world. It conducts research and investigations into government and corporate surveillance activities with a focus on the policies and technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in courts around the world. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional, and international laws that protect this fundamental right. As a part of this mission, Privacy International works with various partner organisations across the world to identify and address threats to privacy.

2. Privacy International wishes to bring its concerns about the protection and promotion of the right to privacy by New Zealand before the Human Rights Council for consideration in New Zealand's upcoming review. This stakeholder focuses on the Government Communications Security Bureau ("GCSB"), New Zealand's foreign intelligence agency, and its activities in relation to non-New Zealanders. It highlights two areas of particular concern:

    - The legislation governing the GCSB explicitly sets a lower standard for non-New Zealanders in relation to surveillance activities, including by permitting surveillance without judicial involvement, in contravention of international human rights standards.
    - Through the GCSB, New Zealand has engaged in practices—including mass surveillance of small Pacific island nations—that violate international human rights standards, largely as part of its participation in the "Five Eyes" intelligence-sharing arrangement with the United States, United Kingdom, Canada, and Australia.

The Right to Privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.[2] It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information, and association. Activities that restrict the right to privacy, such as surveillance and censorship,

[1] Privacy International would like to thank the International Human Rights Clinic at Harvard Law School for its support in the research, preparation, and drafting of this submission.

[2] Universal Declaration of Human Rights, art 12; International Covenant on Civil and Political Rights, art 17; United Nations Convention on Migrant Workers, art 14; Convention on the Rights of the Child, art 16; African Charter on the Rights and Welfare of the Child, art 10; American Convention on Human Rights, art 11; African Union Principles on Freedom of Expression, art 4; American Declaration of the Rights and Duties of Man, art 5; Arab Charter on Human Rights, art 21; European Convention for the Protection of Human Rights and Fundamental Freedoms, art 8; Johannesburg Principles on National Security, Free Expression and Access to Information; Camden Principles on Freedom of Expression and Equality.

can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[3] These requirements apply regardless of the location or nationality of the individual or group whose communications are under surveillance.[4]

4. As innovations in information technology have enabled previously unimagined forms of collecting, storing, and sharing personal data, the right to privacy has evolved to encapsulate state obligations related to the protection of personal data.[5] A number of international instruments enshrine data protection principles, and many domestic legislatures have incorporated such principles into national law.[6]

AREAS OF CONCERN

I. The Intelligence and Security Act 2017

5. In 2017, New Zealand consolidated four statutes[7] into the Intelligence and Security Act 2017 (the "Act"), establishing an overarching authorisation and oversight regime for surveillance activities by New Zealand's three intelligence agencies: the GCSB, the New Zealand Security Intelligence Service, and the National Assessments Bureau.

6. In order to carry out an otherwise unlawful activity (such as tapping phone calls),[8] intelligence agencies must first obtain a warrant, usually an "intelligence warrant".[9] The Act sets up two sets of rules around intelligence warrants: one for New Zealand citizens and permanent residents ("New Zealanders"), and the other for foreigners, living outside or inside New Zealand.

    a. For New Zealanders, an intelligence agency must obtain a "Type 1" intelligence warrant, which is issued jointly by a Minister authorised to do so and a Commissioner of Intelligence Warrants.[10] The threshold for issuing a

[3] See Universal Declaration of Human Rights, art 29; Human Rights Committee, General Comment No. 27: Article 12 (Freedom of Movement), 2 November 1999, CCPR/C/21/Rev.1/Add.9; Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988.

[4] See discussion below.

[5] Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy).

[6] See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data; Guidelines for the regulation of computerized personal data files (UN General Assembly Resolution 45/95 and E/CN.4/1990/72). As of January 2018, over 100 countries had enacted data protection legislation and around 40 countries had pending bills or initiatives in the area: David Banisar, "National Comprehensive Data Protection/ Privacy Laws and Bills 2018," 25 January 2018, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416.

[7] The New Zealand Security Intelligence Service Act 1969, the Government Communications Security Bureau Act 2003, the Intelligence and Security Committee Act 1996, and the Inspector-General of Intelligence and Security Act 1996.

[8] "Fact Sheet No. 6: The authorisation framework," Department of the Prime Minister and Cabinet, available at https://www.dpmc.govt.nz/sites/default/files/2017-09/fact-sheet-6-authorisation-framework.pdf.

[9] Intelligence and Security Act 2017, ss 47, 49.

[10] Ibid, ss 55, 57, 60.

warrant requires that either the activity must be "necessary to contribute to the protection of national security" and identifies or protects against specific enumerated harms, such as terrorism or serious crimes originating outside New Zealand; or if the warrant relates to the more amorphous grounds of contributing to New Zealand's international relations or economic well-being, there must be "reasonable grounds to suspect" that targeted individuals are acting on behalf of foreign entities.

b. By contrast, "Type 2" warrants, for foreigners, require only the approval of the authorising minister, and the warrant must merely "enable [the agency] to carry out an activity that is necessary to contribute to the protection of national security or will contribute to the international relations … or economic well-being of New Zealand."[11]

7. Either type of warrant may only be issued if "additional criteria" that incorporate tests derived from human rights law are met. A warrant must be necessary to meet the intelligence agency's statutory functions, and the proposed activity must be "proportionate to the purpose for which it is to be carried out." The agency must also show that that purpose "cannot reasonably be achieved by less intrusive means."[12] Additionally, there must be safeguards in place to ensure that "nothing will be done in reliance on the intelligence warrant beyond what is necessary and reasonable [to perform an agency's statutory functions]", "all reasonably practicable steps will be taken to minimise the impact of the proposed activity on any members of the [New Zealand] public," and information will only be retained, used, and disclosed as provided for in law.[13]

8. Apart from the warranting regime, New Zealanders receive other additional benefits, such as a prohibition on intelligence agencies obtaining information subject to legal privilege,[14] and the right to make complaints to an oversight body, the Inspector-General of Intelligence and Security (a right that foreigners inside New Zealand can also exercise).[15] Legalised discrimination is reflected in the GCSB's (unclassified) Nationality Policy, which outlines the measures the GCSB takes to protect New Zealanders' information when it carries out foreign intelligence activities.[16] There are also separate rules around when Type 1 warrants can be issued on an urgent basis, as against Type 2 warrants.[17]

Discrimination and Lack of Judicial Authorisation

9. States must respect all individuals' rights to privacy without any distinction based on race, language, national origin or other status, whenever individuals

11 Intelligence and Security Act 2017, s 60.
12 Ibid, ss 10, 11, 61.
13 Ibid, s 61
14 Ibid, s 70.
15 Ibid, s 171(2).
16 GCSB, "Nationality Policy," available at https://www.gcsb.govt.nz/assets/GCSB-Documents/GCSB-Nationality-Policy.pdf.
17 Intelligence and Security Act 2017, ss 71 and 72.

are "subject to [the state's] jurisdiction."[18] All persons affected by the state's exercise of "power" and "effective control" are deemed to be within the states' jurisdiction, and are therefore entitled to equal protection.[19] The exercise of "power" and "effective control" over an individual's information amounts to an exercise of jurisdiction by New Zealand, but the Intelligence and Security Act sets a lower standard for non-New Zealanders' information, thereby discriminating on the basis of national origin.[20]

10. Under international human rights standards, determinations concerning communications surveillance must be made by a competent authority (preferably judicial) that is independent and impartial.[21] It could be argued that the Type 1 warrant regime meets this condition, as warrants are issued jointly by a government Minister and a Commissioner for Security Warrants (and each Commissioner must have previously held office as a High Court judge), but the Type 2 regime does not, as a warrant's issuance requires the approval only of a specified government Minister, without the involvement of any judicial or otherwise independent authority.

11. In its 2016 concluding observations on New Zealand, the Human Rights Committee stated that it was "concerned about the limited judicial authorization process for the interception of communications of New Zealanders and the total absence of such authorization for the interception of communications of non-New Zealanders."[22] The Committee concluded that New Zealand "should take all appropriate measures to ensure that … [s]ufficient judicial safeguards are implemented, *regardless of the nationality or location of affected persons*, in terms of interception of communications and metadata collection, processing and sharing,"[23] as well as to bring "the legal framework regulating communications surveillance" into line with the right to privacy. The Committee's concerns, although directed at earlier legislation, remain relevant to the Intelligence and Security Act, which continues to set lower standards for non-New Zealanders and does not involve a judicial authority.

II. Concerning Surveillance Practices

12. New Zealand is openly part of the "Five Eyes" signals intelligence-sharing alliance created by the United States and United Kingdom after the Second

[18] International Covenant on Civil and Political Rights, arts 2, 26.

[19] The right to privacy in the digital age, Office of the United Nations High Commissioner for Human Rights, 30 June 2014, A/HRC/27/37, para 33; Legal Consequences of the Construction of a Wall in the occupied Palestinian Territory, Advisory Opinion, I.C.J. Reports 2004; see also Report of the Special Rapporteur on the right to privacy, A/HRC/34/60, para 29, 24 February 2017.

[20] The right to privacy in the digital age, Office of the United Nations High Commissioner for Human Rights, 30 June 2014, A/HRC/27/37, para 34.

[21] See "Competent Judicial Authority," International Principles on the Application of Human Rights to Communications Surveillance, 2014, available at https://en.necessaryandproportionate.org/.

[22] Human Rights Committee, Concluding observations on the sixth periodic report of New Zealand, CCPR/C/NZL/CO/6, 26 April 2016, para 15. See also Human Rights Committee, Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23 April 2014, para 10.

[23] Human Rights Committee, Concluding observations on the sixth periodic report of New Zealand, CCPR/C/NZL/CO/6, 26 April 2016, para 16 [emphasis added].

World War, which has included Canada, Australia, and New Zealand since the 1950s.[24] Five Eyes members share intelligence, as well as intelligence-gathering methods and techniques.[25] Documents disclosed by former US National Security Agency ("NSA") contractor Edward Snowden indicate that New Zealand, as part of the Five Eyes alliance, has engaged in surveillance contravening international human rights standards.

Mass Surveillance Infrastructure

13. The GCSB operates a satellite communications interception station at Waihopai, near Blenheim,[26] and a high frequency radio interception and direction-finding station at Tangimoana, near Palmerson North.[27] The Waihopai station is capable of both targeted communication interceptions within the Asia-Pacific region[28] and "full take collections" of the content and metadata of communications and internet traffic.[29] An official inquiry confirmed in 2016 that Waihopai can cover satellites that process approximately one billion communications each day.[30]

14. According to the Snowden documents, Waihopai relies heavily on NSA tools and systems to conduct surveillance.[31] These tools include LATENTTHREAT, which breaks satellite signals into individual communications; LEGALREPTILE, which collects text and call metadata; SEMITONE, which monitors fax and voice messages; FALLOWHAUNT, which targets communications sent over small satellites; JUGGERNAUT, which processes intercepted calls from cell phone networks; LOPERS and SURFBOARD, which eavesdrop on phone calls; and XKEYSCORE, which gathers intercepted Internet data.[32]

15. A July 2018 report by the Inspector-General of Intelligence and Security confirmed that, at least until 2015, the Waihopai and Tangimoana stations operated under authorisations to intercept communications made by the GCSB

[24] See Government Communications Security Bureau, "UKUSA allies," available at https://www.gcsb.govt.nz/about-us/ukusa-allies/. See also Richard Norton-Taylor, "Not so secret: deal at the heart of UK-US intelligence," The Guardian, 24 June 2010, available at https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

[25] U.K.–U.S. Communications Intelligence Agreement (as amended on 10 October 1956), art 5, available at http://discovery.nationalarchives.gov.uk/details/r/C11536921.

[26] "Briefing to the Incoming Minister 2017," Minister Responsible for the GCSB and Minister Responsible for the NZSIS, p 25, available at https://www.gcsb.govt.nz/assets/GCSB-Documents/BIM-Redacted.pdf.

[27] "Annual Report 2017," Government Communications Security Bureau, p 30, available at https://www.gcsb.govt.nz/assets/GCSB-Annual-Reports/GCSB-Annual-Report-2017.pdf.

[28] Ryan Gallagher & Nicky Hager, "New Zealand Spies on Neighbors in Secret 'Five Eyes' Global Surveillance," The Intercept, 4 March 2015, available at https://theintercept.com/2015/03/04/new-zealand-gcsb-surveillance-waihopai-xkeyscore/.

[29] David Fisher, "Snowden GCSB revelations: GCSB 'breaking the law' – Russell Norman," New Zealand Herald, 5 March 2015, available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11411730.

[30] Hon Sir Michael Cullen et al, "Intelligence and Security in a Free Society – Report of the First Independent Review of Intelligence and Security in New Zealand," 29 February 2016, para 3.37, available at https://www.parliament.nz/resource/en-nz/51dbhoh_pap68536_1/64eeb7436d6fd817fb382a2005988c74dabd21fe.

[31] Ryan Gallagher & Nicky Hager, "Documents Shine Light on Shadowy New Zealand Surveillance Base," The Intercept, 7 March 2015, available at https://theintercept.com/2015/03/07/new-zealand-ironsand-waihopai-nsa-gcsb/.

[32] Ibid.

Director, and not subject to any type of warrant.[33] The Intelligence and Security Act 2017 limits the Director's power to make authorisations to situations of extreme urgency, suggesting that Waihopai and Tangimoana's activities have since been brought under that Act's warrant regime.[34]

Mass Surveillance of Pacific Islands

16. In 2015, based on Snowden documents, the *New Zealand Herald* and *The Intercept* reported that Waihopai had been indiscriminately intercepting Asia-Pacific communications.[35] An NSA profile showed GCSB spying operations against more than 20 countries, including Vietnam, China, India, Pakistan, and several South American nations.[36] New Zealand had also reportedly been targeting small island nations: Tuvalu, Nauru, Kiribati, Samoa, Vanuatu, the Solomon Islands, Fiji, Tonga, New Caledonia, and French Polynesia.[37] An NSA memo stated that New Zealand's extensive surveillance of the South Pacific provided "valuable access not otherwise available to satisfy US intelligence requirement."[38]

17. In the South Pacific, the GCSB allegedly monitored government ministers and senior officials, government agencies, international organisations, and NGOs in particular.[39] Intercepted data was allegedly shared *en masse* with Five Eyes partners through XKEYSCORE,[40] an NSA system that connects to vast databases of intercepted emails, online chats, and the browsing histories.[41] In 2013, the New Zealand government allegedly used XKEYSCORE to spy on Solomon Islands' government members, including the Prime Minister's chief of staff.[42] The GCSB is also alleged to have targeted several Solomon Islands pro-democracy campaigners in 2012.[43]

33 Government Communications Security Bureau Act 2003 (as amended prior to repeal), s 13 ("Certain interceptions permitted without interception warrant or access authorisation"); see Office of the Inspector-General of Intelligence and Security, "Public Report: Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009-2015," July 2018, para 38, available at http://www.igis.govt.nz/assets/Uploads/GCSB-Intelligence-Activity-re-South-Pacific.pdf.

34 Intelligence and Security Act 2017, s 78.

35 Nicky Hager & Ryan Gallagher, "Snowden revelations / The price of the Five Eyes club: Mass spying on friendly nations," New Zealand Herald, 5 March 2015, available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11411759.

36 Nicky Hager & Ryan Gallagher, "Snowden revelations: NZ's spy reach stretches across globe," New Zealand Herald, 11 March 2015, available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11415172.

37 Ryan Gallagher & Nicky Hager, "New Zealand Spies on Neighbors in Secret 'Five Eyes' Global Surveillance," The Intercept, 4 March 2015.

38 Ibid.

39 Ibid.

40 Ibid.

41 Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet,'" The Guardian, 31 July 2013, available at https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

42 Ryan Gallagher & Nicky Hager, "New Zealand Used NSA System to Target Officials, Anti-Corruption Campaigner," The Intercept, 14 March 2015, available at https://theintercept.com/2015/03/14/new-zealand-xkeyscore-solomon-islands-nsa-targets/.

43 Nicky Hager & Ryan Gallagher, "Special Investigation: Inside one of the SIS's biggest anti-terrorism operations," TV New Zealand, 14 August 2016, available at https://www.tvnz.co.nz/one-news/new-zealand/special-investigation-inside-one-siss-biggest-anti-terrorism-operations.

18. But collection was not always targeted. Former GCSB Director Sir Bruce Ferguson (2006-2011) confirmed in a 2015 radio interview that from 2009 the GCSB had undertaken "full take" collection of South Pacific communications. He analogised "full take" to a fishing expedition, stating: "You cannot these days just individually select people ... you put out a big net, catch stuff, you throw out the stuff you don't want ... and you keep the stuff you do want."[44]

19. On 4 July 2018, the Inspector-General of Intelligence and Security released her official report into complaints stemming from these allegations: she confirmed that the GCSB had carried out "full take" collection of certain communications in the South Pacific and that the GCSB's activities had "included the collection of telecommunications across satellite links," noting that "some Pacific Island nations were largely dependent on satellites" for international connections.[45]

20. The Inspector-General explained that "full take'" was "a phrase GCSB used to describe the storage of all communications data of certain types"[46] or "a shorthand phrase used by GCSB to describe the collection and retention of unselected communications data (of certain types) acquired from particular satellite communications links."[47] She noted that data stored from "full take" collection "[is not] filtered by reference to selectors (e.g. telephone numbers) before being stored," and could be contrasted "with collection that result[s] in storage of 'selected' data, which [is] filtered by reference to selectors."[48]

21. Her perspective was that the GCSB's activities had complied with New Zealand law, as it "provided scope for collection methods such as 'full take'".[49] Although she noted that the GCSB had a duty to destroy irrelevant information and minimise the impact on third parties when it carried out "full take," she observed that "the primary policies relevant to this duty [to minimise the impact on third parties] were those directed at ensuring interception was confined to foreign communications."[50] In other words, directed at the protection of New Zealanders' information.

22. The Inspector-General further confirmed that "some communications collected by GCSB in relation to the South Pacific were shared with its 'Five Eyes' partner intelligence agencies" and that "partner agency personnel with an established need could be granted access to GCSB intercept storage."[51] As a result, "[f]orwarding data to a partner would mean GCSB did not retain complete direct control of it and relied on the partner to apply and audit agreed access

44 "GCSB in mass collection of Pacific data: Ferguson," Radio New Zealand, 6 March 2015, available at https://www.radionz.co.nz/news/national/267923/gcsb-in-mass-collection-of-pacific-data-ferguson.

45 Office of the Inspector-General of Intelligence and Security, "Public Report: Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009-2015," July 2018, paras 124-126.

46 Ibid, para 23.

47 Ibid, para 112.

48 Office of the Inspector-General of Intelligence and Security, "Public Report: Complaints arising from reports of Government Communications Security Bureau intelligence activity in relation to the South Pacific, 2009-2015," July 2018, para 23.

49 Ibid, para 62.

50 Ibid, para 87.

51 Ibid, paras 27 and 120.

restrictions and controls on data use".[52] While New Zealand law may allow such activities, Privacy International believes that they are in violation of applicable human rights standards as noted below.

Spying During WTO Director-General Election

23. In 2013, the New Zealand government allegedly used XKEYSCORE to spy on candidates for the WTO Director-General position, as a senior New Zealand government Minister was contesting the election.[53] The GCSB reportedly intercepted emails from high-profile candidates from Brazil, Costa Rica, Ghana, Indonesia, Jordan, Kenya, Mexico, and South Korea.[54]

24. In June 2017, the Inspector-General published a report examining whether the GCSB had acted unlawfully or improperly in the WTO election.[55] Although she did not comment on the specific allegations, she found that the GCSB's objectives were "sufficiently broad" to allow for "the collection of foreign intelligence to support a New Zealand government minister's bid for leadership" of the WTO.[56] She concluded that while the GCSB had not "rigorously followed" practices and processes to identify whether requests for foreign intelligence were lawful, its actions were nonetheless lawful.[57]

Lack of Necessity and Proportionality

25. International human rights standards require that every communications surveillance determination be made on the grounds that the surveillance is necessary to achieve a legitimate aim and proportionate to the aim pursued.[58] Further, individuals must have realistic avenues to obtain remedies for rights violations.[59]

26. By indiscriminately collecting satellite communications in the Asia-Pacific region across a number of years, the GCSB failed to comply with the principles of necessity and proportionality. As the High Commissioner for Human Rights has stated:[60]

52 Ibid, para 120.
53 Morgan Marquis-Boire at al, "XKEYSCORE: NSA's Google for the World's Private Communications," The Intercept, 1 July 2015, available at https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/.
54 Ryan Gallagher & Nicky Hager, "New Zealand Spied on WTO Director Candidates," The Intercept, 22 March 2015, available at https://theintercept.com/2015/03/22/new-zealand-gcsb-spying-wto-director-general/.
55 Inspector-General of Intelligence and Security, "Report into Government Communications Security Bureau's process for determining its foreign intelligence activity," June 2017, available at http://www.igis.govt.nz/assets/Inquiries/GCSBs-process-for-determining-its-foreign-intelligence-activity.pdf.
56 Ibid, para 127.1.
57 Ibid, para 92.
58 See "Legality," "Legitimate Aim," Necessity," "Adequacy," and "Proportionality," International Principles on the Application of Human Rights to Communications Surveillance.
59 Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, 23 September 2014, A/69/397, paras 49 and 50.
60 The right to privacy in the digital age, Office of the United Nations High Commissioner for Human Rights, 30 June 2014, A/HRC/27/37, para 25.

> Mass or "bulk" surveillance programmes may … be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.

27. In the case of the GCSB's spying in the Asia-Pacific region, the haystack likely comprised the private communications of hundreds of thousands of individuals living in numerous nations. Moreover, there is no real means for foreigners to seek a remedy within New Zealand. This mass surveillance appears to have been carried out not only to advance broadly defined New Zealand interests, but also at the behest of Five Eyes partners. The legal regime governing the GCSB permitted the practice, and the new legal regime likewise allows for the same to take place.

28. The GCSB also spied on the private communications of foreigners around the 2013 WTO Director-General election. Albeit pursuant to a legal framework, this exercise of nakedly political spying was not necessary to achieve a legitimate aim, such as combating serious crime.

RECOMMENDATIONS

29. Although the Intelligence and Security Act 2017 specifies that one of its purposes is to ensure that intelligence agencies perform their functions "in accordance with New Zealand law and all human rights obligations recognised by New Zealand law",[61] it contains a discriminatory framework and allows for practices that do not meet human rights standards. The GCSB's differing policies in relation to New Zealanders and foreigners, "full take" practices, and political spying contravene international human rights standards. Its practice of sharing information with its Five Eyes partners—and inability to control how that information is used—compounds these human rights violations.

[61] Intelligence and Security Act, s 3(c)(i).

30. To better protect the right to privacy, we recommend that the government of New Zealand take all necessary measures to ensure that its surveillance activities, both within and outside the New Zealand, conform to its obligations under international human rights law, particularly the right to privacy. These measures should include:

    - Reforming the Intelligence and Security Act 2017 to ensure that:
        - Any decision to intercept or interfere with communications, including of metadata, requires involves a judicial authority;
        - The same regime applies to non-New Zealanders as to New Zealanders;
        - Non-New Zealanders have access to an effective remedy for rights violations;
        - All surveillance activities meet the requirements of necessity and proportionality.
    - Reviewing the practice of intelligence sharing with foreign agencies to ensure its compliance with the right to privacy.