Access Now submission to the United Nations Human Rights Council, on the Universal Periodic Review 2018 Cycle for New Zealand

About Access Now

1. Access Now (www.accessnow.org) is an international organisation that works to defend and extend digital rights of users globally. Through representation in 10 countries around the world, including engagement with stakeholders and policymakers from all 8 regions of the world, Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. We engage with an action focused global community, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.
2. Access Now advocates an approach to digital security that promotes policies that protect user rights, including privacy and freedom of expression. Access Now has worked extensively on digital rights including on free expression and web blocking, protection of Net Neutrality, and implementation of data protection regulations.
3. The UPR is an important U.N. process aimed at addressing human rights issues all across the globe. It is a rare mechanism through which citizens around the world get to work with all governments to improve human rights and hold them accountable to international law. Access Now is grateful to make this submission.

Domestic and international human rights obligations

4. This is the third Universal Periodic Review for New Zealand, having been reviewed in 2009 and 2014.[1] In 2009 the government received 64 recommendations and accepted 34 in whole or in part.[2] In their second Universal Periodic Review the government received 155 recommendations and accepted 121.[3]
5. New Zealand has signed and ratified the International Covenant on Civil and Political Rights ("ICCPR"), the International Covenant on Economic, Social, and Cultural Rights ("ICESCR"), the International Convention on the Elimination of All Forms of Racial Discrimination, and the Convention on the Elimination of All Forms of Discrimination against Women.[4] On 26 May 1989, New Zealand ratified the First Optional Protocol to

---

[1] UN Human Rights Council General Assembly, "Reports of the Working Group on the Universal Periodic Review: New Zealand," (Universal Periodic Review, 4 June 2009) https://lib.ohchr.org/HRBodies/UPR/Documents/Session5/NZ/A_HRC_12_8%20New%20Zealand_e.pdf; UN Human Rights Council General Assembly, "Report of the Working Group on the Universal Periodic Review: New Zealand," (Universal Periodic Review, 7 April 2014) https://documents-dds-ny.un.org/doc/UNDOC/GEN/G14/131/43/PDF/G1413143.pdf?OpenElement

[2] UN Human Rights Council General Assembly, "Report of the Working Group on the Universal Periodic Review: New Zealand, Addendum," (Universal Periodic Review, 7 July 2009) https://documents-dds-ny.un.org/doc/UNDOC/GEN/G09/145/11/PDF/G0914511.pdf?OpenElement

[3] UN Human Rights Council New Zealand Mission, "New Zealand Government Reponse to 2014 UPR Recommendations," (Universal Periodic Review, 2014) https://www.hrc.co.nz/files/5314/2406/1357/New-Zealand-Government-Response-to-2014-UPR-recommendations.pdf

[4] Office of the High Commissioner of Human Rights, "Ratification Status for New Zealand," https://tbinternet.ohchr.org/_layouts/TreatyBodyExternal/Treaty.aspx?CountryID=124&Lang=EN

the ICCPR, which allows for individuals to bring complaints directly to the UN Human Rights Committee after exhausting domestic remedies.[5]

6. Although the country has no formal codified constitution, key rights, including the right to freedom of expression, freedom from discrimination, and rights pertaining to unreasonable search and seizure, are found in the New Zealand Bill of Rights Act.[6] Provisions related to the protection of personal data are found in the Privacy Act, which also establishes the office of the Privacy Commissioner of New Zealand.[7]
7. New Zealand is one of the state members of the Five Eyes Intelligence Partnership, which also includes Australia, Canada, the United Kingdom, and the United States. The partnership facilitates the distribution of information and communications, as well as analysis and determinations, acquired through surveillance operations.[8]

Developments of digital rights in New Zealand

Cybersecurity

8. New Zealand published its first Cyber Security Strategy and Action Plan in 2015, which set out a four-part strategy, including cyber resilience, cyber capability, addressing cybercrime, and international cooperation.[9] The Plan committed to consideration of New Zealand's accession to the Budapest Convention, which was reiterated in the 2016 Annual Report on the Action Plan.[10]
9. The outcomes report from the 2016 Cyber Security Summit in 2016 failed to demonstrate the inclusion of a pluralistic array of voices or recognition of the impact of cybersecurity on individuals.[11] The next Cyber Security Summit will take place in 2018.[12]
10. In 2018, New Zealand's Broadcasting, Communications, and Digital Media Minister, Clare Curran, announced that the Ministry would refresh its Cyber Security Strategy and Action Plan.[13] The full scope of the review is ultimately intended to "assess institutional arrangements for cyber security, collaboration with the private sector, efforts to address

---

[5] Office of the High Commisioner of Human Rights, "Optional Protocol to the International Covenant on Civil and Political Rights," (16 December 1966) https://www.ohchr.org/en/professionalinterest/pages/opccpr1.aspx; "International Covenant on Civil & Political Rights," (New Zealand Ministry of Justice, 11 May 2018) https://www.justice.govt.nz/justice-sector-policy/constitutional-issues-and-human-rights/human-rights/international-human-rights/international-covenant-on-civil-and-political-rights/

[6] New Zealand Ministry of Justice, "New Zealand Bill of Rights Act 1990," (1990, reprint as at 1 July 2013) http://www.legislation.govt.nz/act/public/1990/0109/latest/DLM224792.html

[7] New Zealand Ministry of Justice, "Privacy Act 1993," (1993, Reprint as at 21 December 2017) http://www.legislation.govt.nz/act/public/1993/0028/232.0/DLM296639.html

[8] Justin Pemberton, Director, "iSpy (With My Five Eyes)," (2016) https://ispydoc.com/select

[9] "New Zealand's Cyber Security Strategy 2015 Action Plan," https://www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf

[10] Simon Bridges, "New Zealand's Cyber Security Strategy 2016 Action Plan Annual Report," https://www.dpmc.govt.nz/sites/default/files/2017-06/nzcss-action-plan-annual-report-2016.pdf

[11] "New Zealand Cyber Security Summit 2016 Report," (May 2016) https://www.connectsmart.govt.nz/assets/Uploads/Summit-Report-FINAL.pdf

[12] "NZ Cyber Security Summit Event Page," https://www.conferenz.co.nz/events/nz-cyber-security-summit

[13] Paul McBeth, "NZ must step up international cyber-security," (New Zealand Herald, 12 April 2018) https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12031395

cybercrime, system-wide leadership of government information security, international cyber cooperation and responses, opportunities to grow the cyber security sector, and the security challenges of emerging technology."[14] The announcement once again referenced the Budapest Convention and called for the Cabinet to consider pursuing New Zealand's accession.[15]

11. In 2017, in response to a letter sent by Access Now, InternetNZ, and other domestic and international experts and organizations, New Zealand's Attorney General, Hon Christopher Finlayson QC committed to participating in a meeting with relevant stakeholders on the use of encryption and digital security more generally.[16] The United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression found in 2015 that encryption deserves strong protection in that it enables individuals to exercise their human rights.[17]

Data Protection, Privacy, and Government Surveillance

12. In March 2017, the Intelligence and Security Act of 2017 received royal assent.[18] The law replaced previous intelligence laws to create a single system governing separate government agencies.[19] Among other things, the law allows for "purpose-based" warrants that would not need to be tied to any particular person or organization, which would fail to meet a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application.[20]
13. New Zealand's Human Rights Commission published, "Privacy, Data and Technology: Human Rights Challenges in the Digital Age" in May 2018.[21] Among other things, the report set out New Zealand's legal and policy framework regarding privacy and surveillance as well as detailed necessary safeguards for human rights. The report stated, "In terms of human rights obligations, security agencies must not cooperate with

---

[14] Clare Curran, "Refresh of New Zealand's Cyber Security Strategy and Action Plan," (National Cyber Policy Office Proactive Release, April 2018) https://www.dpmc.govt.nz/sites/default/files/2018-04/ers-18-paper-refresh-of-new-zealands-cyber-security-strategy-and-action-plan_1.pdf

[15] *Id*.

[16] "Response of Hon Christopher Finlayson to Access Now, Internet NZ, etc." (7 Aug 2017) https://www.accessnow.org/cms/assets/uploads/2017/10/2017-08-07-Ben-Creet.pdf

[17] Office of the High Commissioner of Human Rights, "Report on encryption, anonymity, and the human rights framework," https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[18] New Zealand Parliament, "Intelligence and Security Bill," (2017) https://www.parliament.nz/en/pb/bills-and-laws/bills-proposed-laws/document/00DBHOH_BILL69715_1/intelligence-and-security-bill ("This bill implements the Government response to the Report of the First Independent Review of Intelligence and Security in New Zealand: Intelligence and Security in a Free Society, and replaces the four Acts that currently apply to the GCSB, the NZSIS, and their oversight bodies.").

[19] "New Zealand: Security and Intelligence Bill Introduced," (Library of Congress, 16 August 2016) http://www.loc.gov/law/foreign-news/article/new-zealand-security-and-intelligence-bill-introduced/

[20] Isaac Davison and Nicholas Jones, "New law targets people who leak classified information," (New Zealand Herald, 15 August 2016) https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11694279; *See also* "International "Principles on the Application of Human Rights to Communications Surveillance," (Necessary and Proportionate, May 2014) https://necessaryandproportionate.org/principles

[21] New Zealand Human Rights Commission, "Privacy, Data and Technology: Human Rights Challenges in the Digital Age," (May 2018) https://www.hrc.co.nz/files/5715/2575/3415/Privacy_Data_Technology_-_Human_Rights_Challenges_in_the_Digital_Age_FINAL.pdf

overseas public authorities where they know or assess that there is a real risk that the activity will lead to, or where information has been obtained as a result of, human rights breaches in that country."[22]

14. A new Privacy Bill was introduced in 2018 for consideration by Parliament. Privacy Commissioner John Edwards has said of the bill, "If the Privacy Bill introduced to Parliament this year becomes law in its current form, New Zealand will have a Privacy Act fit for 2013."[23]

Connectivity and the Gender Digital Divide

15. More than 88% of New Zealand's population uses the internet, well above the region's average of 41.5%. In 2017, New Zealand ranked 13th on the International Telecommunications Union's Information and Communications Technology Development Index.[24] As a region, Asia & the Pacific generally have an internet penetration rate of 47.9% for men and 39.7% for women,[25] though within that region New Zealand generally has a more equal proportion of internet use by gender.[26] In regard to speed, New Zealand ranks 14th in the world on mobile, and 19th on fixed broadband as of May 2018.[27]
16. A 2017 global survey conducted by Amnesty International found that approximately 1 in 3 women surveyed had experienced online abuse and harassment, with 49% of those women who responded affirmatively saying they the experience caused them to fear for their physical safety.[28] 46% reported that the abuse or harassment was "misogynistic or sexist in nature."[29]

Human Rights in the Digital Age

17. Following the Digital Nations 2030 Conference and the D5 Ministerial Conference in February 2018, the Honorable Clare Curran announced that New Zealand would lead the D7, "a network of the world's most advanced digital nations with a shared goal of harnessing digital technology and new ways of working to improve citizens' lives,"[30] in order to "to create a multi-national framework for digital rights."[31] It is not yet clear what form that framework will eventually take or who will be consulted during its development.

---

[22] *Id*.
[23] Katie Kenny, "All you need to know about the proposed privacy laws," (Stuff, 23 May 2018) https://www.stuff.co.nz/national/104126249/all-you-need-to-know-about-the-proposed-privacy-laws
[24] ICT Development Index 2017: New Zealand, https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&NZL https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017comparison-tab
[25] "ICT Facts and Figures 2017", (International Telecommunications Union, 2017), https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
[26] *Id*.
[27] "Speedtest Global Index," (Speedtest, June 2018), http://www.speedtest.net/global-index/
[28] "One in three NZ women harrassed online - survey," (RadioNZ, 20 November 2017), https://www.radionz.co.nz/news/national/344259/one-in-three-nz-women-harrassed-online-survey
[29] *Id*.
[30] "D7 group of digital nations," (Digital Government New Zealand), https://www.digital.govt.nz/digital-government/international-partnerships/d7-group-of-digital-nations/
[31] Clare Curran, "Leading digital nations put digital rights at the heart of their agenda," (Beehive, Official Website of the New Zealand Government, 22 February 2018),

18. According to a survey conducted by New Zealand's official data agency, NZ Tatauranga Aotearoa, "freedom, rights, and peace" is one of the top social characteristics people identify with New Zealand.[32] This data also indicates that "Information Media and Telecommunications" has the second highest gross domestic product across sectors, ranking just behind "business services."[33]

Violations of human rights

19. In 2014, documents made available by Edward Snowden revealed that New Zealand had implemented a mass metadata surveillance program. To do this, the government used a 2013 law that authorized the Government Communications Security Bureau ("GCSB") to collect data on residents and citizens. When the law was passed, then Prime Minister John Key stated that the law was merely designed to fix a legal loophole, and assured the public it "isn't and will never be wholesale spying on New Zealanders."[34] This surveillance program code-named "Speargun" involved the covert installation of cable access equipment on the country's main undersea cable, the Southern Cross Cable, which carries the majority of internet traffic between New Zealand and the rest of the world. They then extracted metadata from communications in real time.[35]
20. In November 2017, an investigation by the New Zealand Herald revealed that Prime Minister Key had knowingly misrepresented the termination date of Speargun. When asked about the program on the eve of his 2014 election he indicated it was discontinued the previous year, approximately 6 months prior to when funding was actually halted.[36] In response to the revelation, Government Communications Security Bureau Minister Andrew Little said he was "personally very uncomfortable" with the idea of mass surveillance, though he supported both Speargun and its successor program.[37]
21. Documents made available by Edward Snowden also showed that New Zealand carried out mass surveillance of several Pacific island states, including Fiji, Papua New Guinea, the Solomon Islands, Nauru, Samoa, Vanuatu, Kiribati, Tonga and French Polynesia. This included monitoring international organizations and NGOs in these. This data was

---

https://www.beehive.govt.nz/release/leading-digital-nations-put-digital-rights-heart-their-agenda (The addition of Canada and Uruguay at the Ministerial Conference caused the change in name from D5 to D7.)

[32] "Society," (New Zealand Stats, 2017) https://www.stats.govt.nz/topics/society

[33] "Economy," (New Zealand Stats, 2017) https://www.stats.govt.nz/topics/economy

[34] Glenn Greenwald and Ryan Gallagher, "New Zealand Launched Mass Surveillance Project While Publicly Denying It," (The Intercept, 15 September 2014) https://theintercept.com/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/

[35] *Id.*

[36] David Fisher, "John Key, mass surveillance and what really happened when Edward Snowden accused him of spying," (NZ Herald, 28 November 2017) https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11948852

[37] David Fisher, "GCSB minister Andrew Little on mass surveillance and our spies obeying the law," (NZ Herald, 1 December 2017) https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11950968

shared with the other Five Eyes members through the documented "X KEYSCORE" surveillance tool.[38]

22. Court documents published in September 2017 revealed that the New Zealand Police had continually monitored and recorded phone calls and texts of prison abolitionist activists for an unknown period of time starting in November 2016 pursuant to the Search and Surveillance Act 2012.[39] These activists were charged with trespass following a demonstration, though they were discharged without conviction. There is no indication that the activists were a security threat.
23. After publishing his book *Dirty Politics* in 2014, which exposed morally questionable behavior of prominent politicians and government officials to attack and discredit the opposition, police sought and received a warrant to raid investigative journalist Nicky Hager's house. In the raid, they seized equipment, 10 months of bank records, travel history, and his daughter's phone records. In December 2015, the High Court ruled that the raid was illegal, and the police were ordered to pay damages to Hager.[40]
24. In 2018, New Zealand Police issued a formal apology in 2018 for their search of Nicky Hagen's house, including for conducting it pursuant to an unlawful, overbroad search warrant and disregarding journalistic privilege in order to identify a confidential source.[41] In apology, the Police noted that behavior during the search constituted "breaches of Mr Hager's legal right to protect his sources and should not have occurred."

Recommendations

25. Cybersecurity and human rights are mutually reinforcing objectives. New Zealand should incorporate human rights protections at the center of its renewed cybersecurity policy. This means, in updating its policy, New Zealand should incorporate user protections throughout each stage of the process and focus on systemic solutions that address the array of risks online. New Zealand should commit to effective participation of all stakeholders throughout the process, including independent experts and members of civil society. Any commitment must ensure equitable access to documents and decision-makers as well as designated opportunities for input and reporting.
26. In planning and preparations for the 2018 Cyber Security Summit, New Zealand should commit to providing meaningful access and opportunities for engagement for civil society and members of the public.
27. Authorities' online surveillance practices must be limited in scope to protect human rights. Protections must be established in law to ensure that international cooperation

---

[38] Nicky Hager and Ryan Gallager, "Snowden revelations/The Price of the Five Eyes club: Mass spying on friendly nations," (NZ Herald, 5 March 2015) https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11411759

[39] Tess McClure, "Members of a prison protest group say they "feel absolutely violated" after learning their phone communications were spied on by police," (Vice, 28 September 2017) https://www.vice.com/en_nz/article/gy5wy9/police-are-tapping-the-phones-of-nz-human-rights-activists

[40] Bryce Edwards, "Political roundup: Dirty Politics won't die," (NZ Herald, 19 December 2015) https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11563693

[41] Felix Geiringer, "Police apologise to Nicky Hager," (Scoop, 12 June 2018) http://www.scoop.co.nz/stories/PO1806/S00109/police-apologise-to-nicky-hager.htm

with other governments -- whether or not facilitated through accession to the Budapest Convention -- meets human rights standards for privacy.

28. The growth of New Zealand's digital economy and the high percentage of New Zealand's population using the internet makes digital security a pressing issue. New Zealand should publicly commit to protecting digital security, including the strongest forms of encryption available, and should encourage and invest in the future of encryption for all forms of digital storage and communications.
29. The New Zealand government holds an important global position as a member of the Five Eyes.[42] Within the Five Eyes, New Zealand should commit to leading on issues of human rights, in line with statements from the Human Rights Commission. Entities within the Five Eyes, including the United Kingdom and the United States, have implemented new and expanded surveillance authorities, including authorities for mass surveillance. New Zealand should publicly endorse the International Principles on the Application of Human Rights to Government Surveillance and encourage other Five Eyes governments to do so as well.
30. In order to implement the safeguards identified in the International Principles on the Application of Human Rights to Communications Surveillance, New Zealand should establish a working group, either within the Human Rights Commission or independently, on how to implement the Principles into law as substantive protections, including as an update to the Intelligence and Security Act of 2017.
31. Mass surveillance is intrinsically inconsistent with human rights. New Zealand should revisit the Intelligence and Security Act of 2017 to strike the authorization for purpose-based warrants to the extent they allow for surveillance unrelated to a specific crime or threat.
32. With the growth of the internet of things coming at the same time as more government and commercial services move online and bring personal data along with them, it is imperative that New Zealand update its data protection laws. These laws must take notice of both the volume and breadth of data and devices connected to the internet and provide meaningful rights and remedies for misuse, abuse, or breaches of that data.[43]
33. Policymakers should engage a broad range of stakeholders in relation to the enforcement of current regulations, in order to protect vulnerable communities from future offenses. The government should also develop policies to punish the perpetrators and to provide the victims with remedies, including psychological, economic, and social resources. Further, law enforcement and judicial agencies should invest in training staff on how to handle gender violence cases.
34. In pursuing a "multi-national framework for digital rights," New Zealand and the rest of the D7 must recognize that human rights apply online as they do offline. The D7 should

[42] "Necessary and Proportionate International Principles on the Application of Human Rights to Communications Surveillance," (Necessary & Proportionate, May 2014) https://necessaryandproportionate.org/principles

[43] For one suggestion, *see* Amie Stepanovich, "Data Protection in the United States: Where do we go from here?" (Access Now, 23 APril 2018) https://www.accessnow.org/data-protection-in-the-united-states-where-do-we-go-from-here/

commit to providing meaningful access and opportunities for engagement for civil society and members of the public in the creation of this framework.

35. The New Zealand Human Rights Commission should report on any outcomes from the court's decision and subsequent apology in the case of Nicky Hagan, including any new safeguards implemented to protect against similar overreach in the future.
36. New Zealand should report on its progress in implementing the recommendations of the UN General Assembly and the UN Human Rights Council in resolutions on the right to privacy in the digital age, including the recommendation to respect human rights in accordance with the UN Guiding Principles on Business and Human Rights.[44]
37. For additional information, please contact Access Now Global Policy Counsel Amie Stepanovich (amie@accessnow.org).

[44] "Privacy, Data, and Technology: Human Rights Challenges in the Digital Age," (New Zealand Human Rights Commission, May 2018) https://www.hrc.co.nz/files/5715/2575/3415/Privacy_Data_Technology_-_Human_Rights_Challenges_in_the_Digital_Age_FINAL.pdf