Discriminatory Surveillance: Who is a New Zealander?

Since the inception of the modern New Zealand Intelligence Community, there has been an ability, solidified in legislation, to conduct surveillance on 'New Zealanders' and 'non-New Zealanders'. Targeting surveillance in this way may have been appropriate before the introduction and ubiquity of the internet and the birth of the digital identity. However, in 2020 the approach focusing on citizenship or even permanent residency of people is discriminatory and potentially creates a massive overcollection of data.

The Intelligence and Security Act, introduced in 2017 enables both the Government Communications Security Bureau and the New Zealand Security Intelligence Service to get surveillance warrants on New Zealanders (under Type 1 warrant) and non-New Zealanders (under a Type 2 warrant), with different approval regimes for each warrant type. It should be noted that obtaining Type 2 warrant does not require judicial authorization which was criticized by the United Nations Human Rights Committee.[1]

With almost 4.5 billion people in the world accessing the internet[2] people's communication isn't occurring on a one-to-one basis. We use many internet-enabled devices. This poses a challenge for the modern surveillance apparatus as any communications device used by a person must be determined to be either a New Zealander or non-New Zealander. How is an IP address (internet address) of a device designated under the legislation? What if one IP address serves to origin communication for a flat of different people? What about a Bluetooth connected bed with a New Zealander and a non-New Zealander using it? Or, so widely used personal voice assistants that may recognize many voices and serve many people? These devices could all be important sources of intelligence information, but it is impossible to understand whether they would be classified as New Zealanders or non-New Zealanders. This is problematic because of the different approval regimes for each warrant type; the surveillance may massively over collect data and even circumvent the right warranting process depending on whether your device is considered a New Zealander or not.

The way the legislation is written and the hidden decision-making process leaves too much power to the intelligence community to make decisions about people's identities. In a time when the new European, New Zealand and Californian privacy regulations empower people to make decisions about their personal information and identity, should New Zealand settle for such outdated legislation and conceptions of identity for their intelligence community? Should someone's human rights depend on the fact that their resident visa is not a permanent one? Aren't human rights for all human beings, after all?

This short article is the first part in a series that will be posted over the next few months outlining the Privacy Foundation's concerns around surveillance in New Zealand and across the Five Eyes alliance.

Contributed by the Surveillance Working Group

---

[1] Human Rights Committee, Concluding Observations on the sixth periodic report of New Zealand (CCPR/C/NZL/CO/6),31 March 2016 at 4.

[2] https://www.statista.com/statistics/617136/digital-population-worldwide/