Position on 'International statement - End-to-end encryption and public safety' of 12 October 2020 drafted by representatives from the UK, US, Australia, New Zealand, Canada, India and Japan.[1]

Privacy Foundation New Zealand

Privacy in the Internet Economy Working Group

5 November 2020

The Statement on the use of end-to-end encryption on digital platforms, signed by the Hon Andrew Little on behalf of the New Zealand government, marks change in New Zealand's approach to this complex issue. While the Statement acknowledges the important role that encryption plays in keeping New Zealanders' digital information safe from a variety of cybersecurity threats, its call to address "the challenges posed by end-to-end encryption" and other applications of encryption technology needs to be carefully reviewed and validated with the New Zealand public. This Position Paper considers the Statement and shares some of the Privacy Foundation's thinking on this topic.

We are pleased to see that the Statement emphasises the crucial role of strong encryption in protecting data and privacy of individuals. This position stands in contrast to the other signatories' view on strong encryption. For example, in 2018 Australia passed legislation[2] that permits the police to require companies to create a 'backdoor' so they can view encrypted communications during an investigation. The legislation has been criticised for being inadequately debated and poorly drafted.[3] In the United States, the Federal Bureau of Investigation has unsuccessfully attempted to require Apple to provide tools for bypassing the security restrictions on iPhones belonging to suspects.[4] We encourage the New Zealand government and the other signatories to maintain the integrity of encryption when exploring ways to gain access to encrypted content for lawful purposes. Undermining encryption will affect more than individuals' data privacy. It will reduce confidence in e-commerce, independent journalism, whistleblowing and many other sectors or scenarios where the confidentiality and integrity of information is essential. For example, it may be a direct threat to vulnerable communities (like LGBTQ) and to groups that oppose authoritarian regimes across the globe.

---

[1] "International statement—End-to-end encryption and public safety" The Beehive <www.beehive.govt.nz>.
[2] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth).
[3] E.g. Keiran Hardy "Australia's encryption laws: Practical need or political strategy?" (2020) 9 Internet Policy Review 1; also, Jon Porter "Australia's encryption-busting law is 'deeply flawed,' says tech industry" (7 December 2018) The Verge <www.theverge.com>.
[4] Brian Barrett "The FBI Backs Down Against Apple—Again" (10 May 2020) Wired <www.wired.com>.

A concern that we have with the Statement is its presentation of access to encrypted communication within the emotional and sensitive context of protecting children from sexual exploitation. Since the popularisation of the Internet, the privacy of its users has been challenged to supposedly prevent the Internet becoming a safe harbour for 'drug-dealers, money-launderers, terrorists and paedophiles'.[5] Such discourse creates a false illusion that everyone who stands for privacy also supports individuals who use the Internet for these sorts of illegal activities. This is, of course, not the case and we agree that law enforcement agencies need to have tools and processes to protect individuals and vulnerable groups in society. As we observed previously, undermining strong encryption is more likely to endanger vulnerable groups in society rather than protect them. Therefore, we encourage the signatories to engage in a less emotional and more solution-oriented discussion with technology, industry and society. Consideration must also be given to existing or alternative solutions that are addressing problems such as the sexual exploitation of children without compromising the integrity of encryption, such as the Digital Child Exploitation Filtering System (DCEFS) managed by the Department of Internal Affairs.[6]

In light of this, we note the Statement does not present any practical proposal for achieving the aim of maintaining public safety while protecting privacy and cybersecurity through encryption. The dilemma that this presents is well known; if technology companies establish a 'backdoor' into their service or technology for law enforcement agencies, it is a matter of time before this 'backdoor' is exploited by malicious actors such as hackers, organised crime and state-sponsored groups. Rather than increasing pressure on technology companies through statements such as this one, we encourage the signatories to invest in collaborative efforts with the technology sector to carefully understand what each of the stakeholders requires and how to achieve these needs without compromising the privacy and cybersecurity of these companies' users. For example, Andrew Woods from the Hoover Institution at Stanford University notes that 'far from going dark, some suggest that this is in fact the golden age of surveillance'. Law enforcement agencies may have a number of alternative means of accessing digital content that does not require them to break encryption through exploiting vulnerabilities in an individual's device or tracking their online activities to glean further information.[7]

Finally, we are concerned that the New Zealand government has signed the Statement without wider public consultation or discussion. This is critical in light of the direct impact that undermining encryption would have on New Zealanders' privacy and cybersecurity. New Zealanders are generally consumers of digital services provided by overseas companies, so the government must consider alternatives and the wider implications of weakening important cybersecurity measures such as encryption before supporting international initiatives such as this Statement.

The Statement shows that the government and the other signatories understand the importance of strong encryption. We invite them to back up their words with actions, investing time and effort into thoroughly understanding the implications for New Zealanders of weakening encryption and proposing meaningful methods to support law enforcement agencies without undermining the security of all.

---

[5] See 8.3.4, Timothy C May "Cypherpunks FAQ" (10 September 1994) <http://groups.csail.mit.edu>; and the example of that argumentation in Scott Pelley "FBI director on privacy, electronic surveillance" <www.cbsnews.com>; or, Adam Bienkov "David Cameron: Twitter and Facebook privacy is unsustainable" politics.co.uk <www.politics.co.uk>.

[6] 'Censorship DCEFS' Department of Internet affairs <www.dia.govt.nz/Censorship-DCEFS>.

[7] Andrew Keane Woods "Encryption Substitutes" (2017) 1705 Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper.

About the Privacy Foundation New Zealand

The Privacy Foundation New Zealand was established in 2016 to protect New Zealanders' privacy rights, by means of research, awareness, education, the highlighting of privacy risks in all forms of technology and practices, and through campaigning for appropriate laws and regulations. Its membership has a diverse range of professional, academic and consumer backgrounds and the Foundation regularly lends its collective expertise to comment on proposed regulation or programmes in the media or by participating in consultation processes.