Australia using new decryption powers even before planned review

8 February 2019, by Max Blenkin

Under the fresh rules, refusal to grant Australian authorities access to devices is punishable with up to 10 years in prison

Australian security agencies have begun using sweeping new powers to access encrypted communications even before a promised review meant to address concerns from the likes of Google, Apple and Facebook.

The powers were granted under a new decryption law which was rushed through parliament in December amid fierce debate, and seen as the latest salvo between governments worldwide and tech firms over national security and privacy.

Two months later, the Australian Federal Police have revealed that agents have already used it while investigating drug trafficking and child exploitation.

Australia is widely seen as a global test case for such laws, with possible applications by other governments seeking to counter the growing use of encrypted messaging, notably Australia's partners in the so-called "Five Eyes" intelligence alliance—the United States, Britain, Canada and New Zealand.

Under the new laws, refusal to grant authorities access to devices is punishable with up to 10 years in prison, and police told a parliamentary inquiry they had used that threat to compel two suspects to hand over their passwords.

Citing secrecy provisions in the law, police declined to say if they had used it to force device makers or telecommunications firms—including global giants such as Apple—to break or bypass encrypted communications.

The same provisions bar companies from disclosing whether they have received such police demands, known as "compulsory notices".

The government has argued the law was urgently needed to foil terrorist plots and intercept communications among other serious criminals.

But opponents allege it punches a hole in global efforts to keep governments from eavesdropping on secure communications, such as WhatsApp.

They also argue it could undermine legitimate uses of encryption for commerce and banking, saying you cannot create vulnerabilities in encryption technologies without opening the door for them to be used by malicious actors.

"That is a needle that cannot be threaded—you cannot break encryption without introducing a vulnerability into the whole system," an alliance of tech giants, including Amazon, Google and Facebook, said in a submission about the legislation before it was adopted in December.

Threat to industry

The legislation was passed only after the conservative government agreed to reopen debate in the new year on amendments that would address

widespread concerns among civil liberties advocates and tech industry experts that it was ill-conceived and too broad.

The Department of Home Affairs says the law is being progressively implemented and that in January it wrote to tech industry members for assistance in drawing up guidelines on how to use the new powers.

But the tech industry appears far from reassured.

"There is no doubt there is an extremely broad coalition of stakeholders that are very concerned about the impact of this bill," said John Stanton, chief executive of the Communications Alliance, which represents the Australian communications industry.

"It is not just industry, it is civil society and digital rights activists (too)."

Stanton warned the new law posed "an enormous threat" to export opportunities for Australian tech firms "because they can no longer provide any assurance that their gear hasn't been tampered with by Australian security".

"Even to say, 'no, it hasn't', is an offence" under the law," he added.

Industry groups have combined forces to present a joint submission to the latest inquiry proposing a series of amendments.

These include a higher threshold for using the law, which can currently be applied in any investigation of an offence carrying a maximum three-year jail term—a bar critics say is too low.

The industry also wants more precision about an element of the law barring authorities from forcing companies to introduce a "system vulnerability" into their products—a term they say is ambiguous.

The tech industry alliance warned the new law as written could force companies to take actions in Australia that violate laws in other nations where they operate or have clients.

And they issued a thinly veiled warning that the law could force major global companies to end or restrict their activities in Australia.

"Australians may not have access to the best technology, because technology providers may choose not to sell to Australians and submit to this legislation," the alliance said in its submission to parliament.

The parliament committee must complete its review by April 3, but any moves to then amend the legislation risk running up against the Australian electoral cycle, with a federal poll due by mid-May.