14 SEP, 2019
Hidden surveillance
New Scientist, National

News Insight

Privacy

Hidden surveillance

Australia's anti-encryption measures have led to widespread concerns over civil liberties, reports **Ruby Prosser Scully**

POLITICIANS around the world are calling for so-called back doors to let them read messages on encrypted chat apps. But the surprising fall-out from Australia's sweeping new encryption regulations reveals that such breaches of privacy can have unexpected consequences.

During her time as UK prime minister, Theresa May repeatedly called for tech companies to provide her government with ways to access encrypted messages, believing that terrorists were using them to communicate.

This sentiment hasn't gone away. In late July, the UK's new home secretary Priti Patel said messaging apps shouldn't "empower criminals" by providing a sealed-off means of communication. Meanwhile, the Trump administration in the US reportedly met recently to debate whether to ban methods of encryption that law enforcement can't break.

But in Australia, a law approved by parliament in late 2018 has raised strong privacy concerns, without much evidence that the introduced measures have helped thwart any crime. Leaders of other nations looking to manage encryption would do well to study the country's cautionary tale.

REUTERS/THOMAS WHITE

Telegram gives users the option of using end-to-end encryption

Encryption is a mainstay of digital services like online shopping, email and messaging apps. It means that information is scrambled unless your device has the cryptographic key.

JASON REED/REUTERS

Tech firms in Australia say their products could be seen as less secure

A form of this technology called end-to-end encryption has gained popularity in the past few years. Offered by apps like WhatsApp and Telegram, it means that messages are never stored in a decrypted form by the service provider, so they can't ever read them. That is a strong draw for some privacy-minded individuals.

"These services are designed from the beginning so that the service provider doesn't know what is being communicated," says Vanessa Teague at the University of Melbourne, Australia.

Nevertheless, governments want a back door into such systems. This was the impetus for the most controversial part of Australia's new law, the Assistance and Access Act. It gives law enforcement and intelligence agencies three main powers.

First off, they can ask tech firms to help them access a user's communications. If the company doesn't want to, the agency can compel them to by issuing a technical assistance notice. If a company says it can't comply because its technology doesn't allow it, then the government can force it to make changes to its service that would allow compliance.

How that works is a matter of debate. One reading of the law is that companies can be forced to hack their own users, for example by installing what is effectively malware to read their messages before they are encrypted (see "Sneaky peeks", left).

In comments submitted to the Australian parliament, Apple said such measures could, for example,

Sneaky peeks

In 2013, Edward Snowden, then working for the US National Security Agency, revealed the details of an agreement between the NSA and several tech companies. The firms gave the agency covert access to their users' messages – a secret back door.

After these revelations, many firms began offering end-to-end encryption, meaning they never store decrypted messages. It is almost impossible to break modern encryption, so these firms can't provide a back door.

But there is a loophole: if someone can access your smartphone, they might be able to sneak a look at messages before they are encrypted.

AUTHOR: Prosser Scully SECTION: GENERAL NEWS ARTICLE TYPE: NEWS ITEM AUDIENCE : 18,909
PAGE: 20 PRINTED SIZE: 1602.00cm² REGION: National MARKET: Australia ASR: AUD 17,438
WORDS: 1253 ITEM ID: 1172152575

14 SEP, 2019

Hidden surveillance

New Scientist, National

"allow the government to order the makers of smart home speakers to install persistent eavesdropping capabilities into a person's home".

The government has said it won't force companies to introduce a "systemic weakness". That phrasing is contentious. It is possible for even subtle changes to computer code to introduce vulnerabilities that hackers can exploit, sometimes without being detected for many years. This means that almost any change that the government forces firms to make could have the potential to endanger people's privacy.

Unsurprisingly, this law has made tech companies concerned over the future of their sector in Australia. Microsoft has said companies it works with are no longer comfortable about storing their data there. And a survey of people working in the country's cybersecurity industry found that the third-highest concern was consumers perceiving their products as less secure thanks to the new law.

Although framed as targeting terrorism, the law's scope includes a range of relatively minor crimes, from white collar offences like copyright infringement to growing and selling marijuana.

An unexpected impact of this has been high-profile searches of journalists' property. For example, in 2018, reporter Annika Smethurst exposed secret emails between Australian public servants discussing a plan to allow the country's cybersecurity agency to covertly monitor citizens. On 4 June, the federal police raided her home and searched her electronic devices to find the source of her story. Police have also raided Australian Broadcasting Corporation offices in Sydney using the same powers.

What tech firms have said about Australia's encryption law:

"This bill could allow the government to order the makers of smart home speakers to install persistent eavesdropping capabilities into a person's home"
Apple

"The underlying assumption of the Act, that a security vulnerability can be created for a targeted technology without creating a systematic weakness or vulnerability, is technically flawed"
Amazon

"The law has created uncertainty for our staff and our customers. It places the tech industry in a chokehold"
Scott Farquhar, co-founder of software firm Atlassian

Previously, police would have required a special warrant to search through a journalist's digital notes. The new encryption law has granted them the power to "add, copy, delete or alter" material that they find on any of a journalist's devices without necessarily having a warrant.

Lizzie O'Shea, a legal expert at Digital Rights Watch, says the new law also gives the police power to install malware on a journalist's phone and get information that way, without anyone knowing. "Who knows what kinds of things are happening under the cover of secrecy," she says.

There are worries that this will have a chilling effect on whistle-blowers and journalism. Riana Pfefferkorn, at the Center for Internet and Society at Stanford Law School in California, wrote to the Australian parliament to make this point in June.

Have the new regulations helped investigate and prevent terrorism? Australia's home affairs minister Peter Dutton has said that the law has played a "very positive role, in a number of investigations".

Yet if people want to get around the law, they may be able to, says David Tuffley at Griffith University in Queensland. For example, they could use services from companies based outside Australia that aren't inclined to comply with the country's rulings.

What can politicians in other countries take from all this? Australia's experience seems to underline that it is extremely difficult to enable a back door into encrypted messages without threatening civil liberties and tech businesses.

Many campaigners in Australia want the law scrapped. "Civil society organisations have been calling for a wholesale repeal of the act," says O'Shea. Failing that, one way to ameliorate the effects would be to require judicial oversight of the powers, she says.

There is some possibility that this could happen. Two reviews of the law are due to report early next year and they may recommend such changes.

Things might play out differently in other countries, because Australia is one of the few liberal democracies without a bill of human rights. If politicians in the UK or US introduced an encryption law, citizens would have human rights legislation as a protective counterpoint. ▮