Australia passes new law to thwart strong encryption



Enlarge / The Member for Sydney Tanya Plibersek speaks as the Labor party stay for the end of parliament in the House of Representatives at Parliament House on December 06, 2018, in Canberra, Australia.

reader comments

30 with 24 posters participating

Share this story

On Thursday, the Australian parliament approved a measure that critics say will weaken encryption in favor of law enforcement and the demands of government.

The new law, which has been pushed for since at least 2017, requires that companies provide a way to get at encrypted communications and data via a warrant process. It also imposes fines of up to A$10 million for companies that do not comply and A$50,000 for individuals who do not comply. In short, the law thwarts (or at least tries to thwart) strong encryption.

Companies who receive one of these warrants have the option of either complying with the government or waiting for a court

order. However, by default, the orders are secret, so companies would not be able to tell the public that they had received one.

“It’s a big deal,” Adam Molnar, a lecturer in criminology at Deakin University in Australia, told Ars.

However, the law as currently written seems to contain what some view as a loophole. The statute says that companies cannot be compelled to introduce a “systemic weakness” or a “systemic vulnerability” into their software or hardware to satisfy government demands.

Those terms are not fully defined in the current law but are set to be added in the forthcoming amendments.

Molnar pointed out that the new law not only implicates his home country but also the other four members of the so-called “Five Eyes” of English-speaking nations, which include New Zealand, Canada, the United Kingdom, and the United States.

The US government (particularly the FBI and Department of Justice) has long complained of the “going dark” problem, but it has not managed to get any adequate federal legislation to address the issue since the failed “Clipper Chip” of the 1990s.

Australian authorities are already known to cooperate with American law enforcement, notably as part of the investigations into the “Love Zone” child-porn website.

“The Government is responding to the impediment that the increasing prevalence of encrypted data and communications represents to available investigative and interception capabilities,” the Australian parliament wrote in its Bill Digest.

“The Bill contains measures aimed at facilitating lawful access to communications and data through two

avenues—decryption of encrypted technologies and access to communications and data at points where they are not encrypted."

"Encryption is simply math"

The law, which takes effect after it is formally approved by the governor-general during a process known as Royal Assent, is expected to be amended almost immediately during the next session of parliament in early 2019.

Silicon Valley has largely decried Canberra's new law. In particular, Apple, which famously resisted American efforts to break its own encryption during a 2015 terrorism investigation, previously told Australian lawmakers that what they are legislating is impossible.

"Some suggest that exceptions can be made, and access to encrypted data could be created just for only those sworn to uphold the public good," Apple continued. "That is a false premise. Encryption is simply math. Any process that weakens the mathematical models that protect user data for anyone will, by extension, weaken the protections for everyone. It would be wrong to weaken security for millions of law-abiding customers in order to investigate the very few who pose a threat."

Even Riana Pfefferkorn—a cryptography expert and attorney at Stanford Law School who submitted formal October 2018 testimony to the Australian parliament arguing against the law—doesn't know what is meant exactly by "systemic weakness."

"Nobody knows!" she said, while laughing for a brief moment. "Whenever you open up a vulnerability in a piece of software or a piece of hardware, it's going to have consequences that are unforeseeable."

https://arstechnica.com/?p=1424613