Tech giants warn Australia against law to break encryption

November 29 2018

Digital giants led by Google, Facebook and Amazon say the proposed Australian law would undermine rather than enhance the nation's security

Digital giants led by Google, Facebook and Amazon have warned Australia against passing a "fundamentally flawed" law allowing security

services to spy on encrypted communications among suspected criminals and terrorists.

In a submission sent to parliament this week and made available to AFP Thursday, the Digital Industry Group Inc (DIGI) said the legislation proposed by Australia's government would undermine rather than enhance the nation's security.

The bill, currently under consideration by a parliamentary committee, would give security agencies wide powers to force telecommunications and technology companies to give them access to encrypted devices and messaging apps.

The conservative government of Prime Minister Scott Morrison has demanded the bill be passed into law before parliament goes into recess on December 6, saying a number of ongoing counter-terrorism investigations were being hindered by plotters' use of encrypted messaging.

Authorities stepped up pressure for the bill's urgent adoption after three men were arrested and charged two weeks ago for allegedly plotting an Islamist-inspired mass shooting attack in Melbourne using encrypted messaging applications to communicate.

The DIGI alliance, which also includes Twitter and Verizon's Oath platforms, said the bill as written would force them to create vulnerabilities in their operations which could be exploited by bad actors.

"Deliberately creating a means of access to otherwise secure data will create weaknesses and vulnerabilities that, regardless of the good intentions at the time, will give an opportunity for other actors –- including malicious ones -– to access that same data," they said.

Firms reject the notion that encryption can be both effective and broken when needed.

"That is a needle that cannot be threaded—you cannot break encryption without introducing a vulnerability into the whole system," the alliance said.

The technology firms further complained that the proposed law did not include enough judicial safeguards against possible abuse by security agencies, and could force them to "take actions in Australia that violate laws of other countries in which they operate or have customers."

The group suggested a series of amendments, including the need for all security agency demands to be approved by an independent judge; that they do not require providers to build weaknesses into their systems or products; or impose "new data retention and interception capabilities".

It also said the demands could not require technology providers to do anything in Australia that would breach laws of other countries.

The DIGI submission noted that the proposed Australian law went significantly further than existing security legislation in the United States or Britain, and would clash with data privacy laws recently adopted in the European Union.

Australia is a member of the so-called "Five Eyes" intelligence alliance along with the US, Britain, Canada and New Zealand, and critics have suggested the new surveillance law could be a test case for toughening anti-encryption efforts in other countries.

The firms issued a veiled warning that adoption of the proposed law could lead major technology 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," they said.