# Australia anti-encryption law rushed to passage

7 December 2018, by Rod Mcguirk And Frank Bajak

Credit: CC0 Public Domain

A newly enacted law rushed through Australia's parliament will compel technology companies such as Apple, Facebook and Google to disable encryption protections so police can better pursue terrorists and other criminals.

Cybersecurity experts say the law, the first of its kind globally, will instead be a boon to the criminal underworld by undermining the technical integrity of the internet, hurting digital security and user privacy.

"I think it's detrimental to Australian and world security," said Bruce Schneier, a tech security expert affiliated with Harvard University and IBM.

The law is also technically vague and seems contradictory because it doesn't require systematic weaknesses—so-called "backdoors"—to be built in by tech providers. Such backdoors are unlikely to remain secret, meaning that hackers and criminals could easily exploit them.

Backdoors were central to a 1990s U.S. effort to require manufacturers to install a so-called "Clipper chip " into communications equipment so the government could listen in on voice and data transmissions. U.S. law enforcement officials, including Deputy Attorney General Rod Rosenstein, are again pushing for legislation that would somehow give authorities access to secure communications.

The Australian bill is seen by many as a beachhead for those efforts because the nation belongs to the "Five Eyes" security alliance with the U.S., Britain, Canada and New Zealand.

"There is a lot here that doesn't make any sense," Schneier said of the Australian bill. "This is a technological law written by non-technologists and it's not just bad policy. In many ways, I think it's unworkable."

A leading figure in cryptography, Martin Hellman of Stanford University, said it appears the bill would "facilitate crime by weakening the security of the affected devices."

The law won final legislative approval late Thursday, parliament's final session of the year. Prime Minister Scott Morrison said it was urgently needed.

"This was very important legislation to give police and security agencies the ability to get into encrypted communications," he told Nine Network television. "Things like WhatsApp, things like that which are used by terrorists and organized criminals and indeed pedophile rings to do their evil work."

He noted that the opposition Labor Party "had to be

dragged to the table" and backed the legislation as an emergency measure out of concern extremists could target Christmas-New Year crowds.

Labor lawmakers they want amendments passed when parliament resumes in February. Opposition leader Bill Shorten said he supported the current bill only because he could not "expose Australians to increased (national security) risk."

Duncan Lewis, director-general of the Australian Security Intelligence Organization, noted during hearings that extremists share encrypted messages that Australia's main secret service cannot intercept or read.

President Morry Bailles of the Law Council of Australia, a leading lawyers' group, criticized the bill's swift parliamentary journey though lawmakers knew "serious problems exist" with giving law enforcement "unprecedented powers to access encrypted communications."

Australian law enforcement officials have complained that the growth of end-to-end encryption in applications such as Signal, Facebook's WhatsApp and Messenger and Apple's iMessage could be the worst blow to intelligence and law enforcement capability in decades. Federal Police Commissioner Andrew Colvin said it hampers criminal investigations at all levels.

But Apple, in comments filed with parliament in October, argued that "it would be wrong to weaken security for millions of law-abiding customers in order to investigate the very few who pose a threat."

The company's iPhones, because of their strong encryption, are bulwarks of national security around the globe and help protect journalists, human rights workers and people living under repressive regimes.

"The iPhone is national security infrastructure right now," said Schneier. "Every Australian legislator uses the systems and devices that that law will target and making them insecure seems like a really bad idea."

Apple also complained in October that the bill was "dangerously ambiguous."

One apparent contradiction confounds technologists. The legislation says the government "must not require providers to implement or build systemic weaknesses in forms of electronic protection ('backdoors')" but also says it can "require the selective deployment of a weaknesses or vulnerability in a particular service, device or item of software on a case-by-case basis."

Technologists say that the mathematics underlying encryption and the manner in which it is encoded into software make it impossible to decrypt a single user's communications without affecting all users.

Eric Wenger, director of cybersecurity and privacy policy for the U.S. technology giant Cisco Systems, warned during debate on the bill that Australia could be at a competitive disadvantage if its data was not regarded as secure.

Australia was a major driver of a statement agreed to at the Group of 20 leaders' summit in Germany last year that called on the technology industry to provide "lawful and non-arbitrary access to available information" needed to protect against terrorist threats.