Australia passes cyber snooping laws with global implications
6 December 2018, by Glenda Kwek

Australia Thursday passed controversial laws allowing spies and police to snoop on the encrypted communications of suspected terrorists and criminals, as experts warned the "unprecedented powers" had far-reaching implications for global cybersecurity.

There has been extensive debate about the laws and their reach beyond Australia's shores in what is seen as the latest salvo between global governments and tech firms over national security and privacy.

Under the legislation, Canberra can compel local and international providers—including overseas communication giants such as Facebook and WhatsApp—to remove electronic protections, conceal covert operations by government agencies, and help with access to devices or services.

Australian authorities can also require that those demands be kept secret.

The conservative government had pushed for the bill to be passed before parliament rises for the year this week, saying the new powers were needed to thwart terror attacks during the festive period.

A last-minute deal was struck with the opposition Labor Party over its demands for more oversight and safeguards when the laws are used, with a review of the legislation to take place in 18 months.

The government also agreed to consider further amendments to the bill early next year.

National cyber security adviser Alastair MacGibbon said police have been "going blind or going deaf because of encryption" used by suspects.

Brushing off warnings from tech giants that the laws would undermine internet security, MacGibbon said they would be similar to traditional telecommunications intercepts, just updated to take in modern technologies.
Global communications firms, including Google and Twitter, have repeatedly said the legislation would force them to create vulnerabilities in their products, such as by decrypting messages on apps, which could then be exploited by bad actors.

A central protection in the laws to block authorities from forcing companies to build a "systemic weakness" into their product remains poorly defined, critics say.

The Law Council of Australia, the peak body for the legal profession, said it had "serious concerns" about the changes.

"We now have a situation where unprecedented powers to access encrypted communications are now law, even though parliament knows serious problems exist," it said in a statement.

Experts such as the UN special rapporteur on the right to privacy Joseph Cannataci have described the bill as "poorly conceived" and "equally as likely to endanger security as not".

"Encryption underpins the foundations of a secure internet and the internet pervades everything that we do in a modern society," Tim de Sousa, a principal at privacy and cybersecurity consultancy elevenM, told AFP.

"If you require encryption to be undermined to help law enforcement investigations, then you are ultimately undermining that encryption in all circumstances. Those backdoors will be found and exploited by others, making everyone less secure," he said.

The new laws also include secrecy provisions, which could raise doubts over whether Australian and foreign vendors have already been compelled to act—undermining their business models where privacy is a key selling point.

The most high-profile clash over security and privacy was between Apple and the US' FBI, when agents sought access to the data of the San Bernardino attackers in California in 2015.