Australia's top spy urges big tech to unravel encrypted chats

April 24 2024

Credit: Pixabay/CC0 Public Domain

Australia's top spy on Wednesday urged greater cooperation from the big tech companies, asking them to break a long-held industry taboo by providing access to encrypted messages.

Intelligence chief Mike Burgess said encrypted messaging had compromised the ability to root out threats, and said tech companies had a duty to break encryption when asked.

"Without their help in very limited and strictly controlled circumstances, encryption is unaccountable," said Burgess, from the Australian Security Intelligence Organisation.

Many tech platforms pride themselves on the ability to guarantee privacy through encrypted messaging channels, and providing access to law enforcement has long been seen as off-limits.

Companies such as Apple, Google and Microsoft have rebuffed similar calls in the past, labeling them a threat to cyber security and user privacy.

"Encryption is clearly a good thing, a positive for our democracy and our economy," Burgess said.

But, he added, "It also protects terrorists and spies, saboteurs and abhorrent criminals".

"I'm asking, urging, the tech companies to work with us to resolve this challenge.

"I'm not asking for new laws. I'm not asking for new powers. I'm asking for the tech companies to do more."

Burgess said intelligence agencies were currently investigating a "racist extremist network" using encrypted messaging.

"Sharing vile propaganda, posting tips about homemade weapons and discussing how to provoke a race war," he said.

Speaking alongside Burgess, Australian Federal Police Commissioner Reece Kershaw singled out Meta, which has been rolling out end-to-end encryption for Facebook and Facebook Messenger.

End-to-end encryption stops law enforcement from intercepting messages, meaning only the sender and recipient are able to read their contents.

Kershaw said this would severely hamper investigations, calling the lack of cooperation with authorities "a disgrace".

Apple notably resisted a legal effort to weaken iPhone encryption to allow authorities to read messages from a suspect in a 2015 bombing in San Bernardino, California.

Police officials worldwide say encryption can protect criminals, terrorists and pornographers even when authorities have a legal warrant for an investigation.

But civil rights and privacy advocates, along with cybersecurity professionals, advocate encrypting data to protect against wrongful snooping by authorities as well as hackers.