SAMUEL HAIG

AUG 27, 2021

'Surveillance state': Australian police given sweeping new hacking powers

Legislation dramatically expanding the hacking capabilities of Australian authorities investigating suspected cybercriminals has been passed through the country's Senate.

10630 19 2:52

Sweeping legislation allowing officials from the Australian Federal Police and Australian Criminal Intelligence Commission to target suspected criminals online has passed through the country's parliament with bipartisan support.

On Aug. 25, the Identify and Disrupt bill passed through Australia's Senate, introducing three new warrants allowing authorities to take unprecedented action against suspected cybercriminals.

The new warrants authorize police to hack the personal computers and networks of suspected criminals, seize control of their online accounts and identities, and disrupt their data.

Home Affairs Minister Karen Andrews praised the broad expansion of powers available to Australian authorities targeting cyber actors. "Under our changes, the AFP will have more tools to pursue organized crime gangs to keep drugs off our street and out of our community, and those who commit the most heinous crimes against children," she said.

While both the government and opposition supported the legislation, Senator Lidia Thorpe of the minor party The Greens slammed the bill for hastening Australia's march down the path to becoming a "surveillance state":

> "In effect, this Bill would allow spy agencies to modify, copy, or delete your data with a data disruption warrant; collect intelligence on your online activities with a network activity warrant; also they can take over your social media and other online accounts and profiles with an account takeover warrant."

"What's worse, the data disruption and network activity warrant could be issued by a member of the Administrative Appeals Tribunal [...] It is outrageous that these warrants won't come from a judge of a superior court," she added.

While 60 amendments were made to the legislation after the Parliamentary Joint Committee on Intelligence and Security (PJCIS)

recommended changes to the legislation, 10 of the security committee's 33 suggestions were ignored.

The amendments added to the bill bolster regulatory oversight of the new measures, include strengthened protections for

recommended that the issuance of warrants be restricted to offenses against national security, including money laundering, serious narcotics, cybercrime, weapons and criminal association offenses, and crimes against humanity. However, the finalized bill does not include amendments that reduce the scope of offenses in this way.

The government has pledged to revisit the PJCIS's recommendations through a broad reform of the intelligence surveillance apparatus.

Related: Australian Hacker Sentenced to 2 Years in Prison for $300K XRP Theft

Shadow Assistant Minister of Cybersecurity Tim Wilson described the PJCIS' rejected recommendations as offering "an important constraint" on authorities exercising the new powers, stating:

> "While we support the bill. [...] Safeguards in this bill could go further, particularly in relation to the offenses this bill applies to."

#Government #Australia #Privacy #Regulation

RELATED NEWS

Bitcoin Price Rally by 2021 Looks Likely From Five Fundamental Factors

One NFT project believes Mars might be the top P2E destination in the metaverse

Anthony Scaramucci: $100K per BTC by year-end is still within reach

Not Legal Advice... America: The world's most creative junkie