AUSTRALIA: 'HACKING BILL' TO WIDEN GOVERNMENT SURVEILLANCE

Pratham Arora, *Consultant*

WHAT IS THE BILL?

Passed in 2021, the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2021, dubbed as the "Hacking Bill", empowers Australian law enforcement agencies, specifically the Australian Federal Police (AFP) and the Australian Criminal Intelligence Commission (ACIC), to use three new types of warrants for digital and tech-based investigation.

- It's called the "hacking" bill because it gives these agencies the power to do that, among other things.
- Agencies can hack the devices of suspected criminals under the powers granted by this bill.
- Furthermore, the bill also says that companies, system administrators and others must actively help the police to modify, add, copy, or delete the data of a person under investigation.
- If they comply, they are protected from civil liability. If they refuse, they could be jailed for up to a decade.

THE THREE WARRANTS

The bill allows law enforcement agencies to employ three types of warrants, as mentioned earlier. These are:

DATA DISRUPTION WARRANT

- This warrant gives the police the ability to "disrupt" the data of a suspect by modifying, copying, adding to, or deleting it. This would be done to prevent the "continuation of criminal activity by participants".

NETWORK ACTIVITY WARRANT

- This warrant would allow law enforcement to collect intelligence from devices or networks that are used, or likely to be used, by those named in it.

ACCOUNT TAKEOVER WARRANT

- It would allow police to take over an online account of a suspect to gather information for an investigation.

- The bill says the first two types of warrants need not be issued by a judge, as a member of the Administrative Appeals Tribunal (ATT) will be sufficient. (ATT is an institution that reviews administrative decisions made by government ministers, departments, and agencies.)
- When presented with any of these warrants, Australian companies and citizens must comply or face up to 10 years in jail.
- This means they must actively help the police change, copy and delete data, intercept and alter communications, spy on networks, and change account credentials of individuals suspected of a crime.

THE ROAD TO PASSAGE

The Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended the passage of the so-called "hacking" Bill earlier in Aug, accompanied with 33 recommendations:

- Deputy Leader of the Opposition Kristina Keneally confirmed in the Senate that the government has implemented "wholly or substantially" 23 of the 33 recommendations through legislative amendments or changes to the Bill's explanatory memorandum.

- These include strengthening the issuing criteria for warrants, including considerations for privacy, public interest, privileged and journalistic information, and financial impacts; reviews by the INSLM (International Security Legislation Monitor) and the PJCIS; sunset powers in five years; and good-faith immunity provisions for assistance orders.

MAJOR RECOMMENDATIONS
An authorising officer must be satisfied that there are no alternative means available to prevent or minimise the imminent risk.
When an issuing authority declines to retrospectively approve an emergency data disruption authorisation, the issuing authority may require the AFP or ACIC to take remedial action, including financial compensation.
The OAIC previously testified the definition of a "criminal network of individuals" is too wide and ambiguous, opening up the possibility of people who are unrelated to a suspicion being under its ambit. Hence, the PJCIS has asked the definition under the network activity warrant to include a reasonable suspicion of a connection.
With regard to authorisation, the committee wants changes made to reflect that only an AFP or ACIC law enforcement officer can apply for a data disruption warrant or an account takeover warrant.

CRITICISMS

When the Bill was passed, Australia's Human Rights Law Centre (HRLC) opined that the Bill had ignored crucial recommendations from the PJCIS. It must be noted that 23 of the 33 recommendations were accepted, while 4 more were accepted to be incorporated into the national security legislation review. **Two of the biggest criticisms of the law are:**

LACK OF SAFEGUARDS

- There is a lack of safeguards in the bill, especially since it could potentially be used against journalists and whistleblowers.
- The PJCIS in turn recommended dozens of changes to the proposed law, including narrower criteria for the use of these powers and stronger oversight.
- "But the [government] has rejected or only partially adopted approximately half of the committee's recommendations and rushed the new law through Parliament," HRLC wrote.

WIDE INTERPRETATIONS

- Another criticism concerns the types of crimes these powers would be used against.
- Home Affairs Minister Peter Dutton said the Bill would only be used for a limited range of criminals, the Bill itself states it can be used to counter all commonwealth offences.
- According to the Green Party, "This Bill enables the AFP (Australian Feferal Police) and ACIC (Australian Criminal Intelligence Commission) to be 'judge, jury, and executioner'.

ASSESSMENT

The powers that the Bill confers to authorities are, unequivocally, far reaching. However, the Minister of Home Affairs is responsible to ensure no abuse of power is exercised. Also, the Inspector General of Intelligence and Security has oversight over the authority granted to police.

Nonetheless, it promotes the expansion of surveillance regime and at the same time, threatens digital rights of Australian people. It grants broad and invasive hacking powers to law enforcement agencies, expanding the scope of government surveillance. It also lacks effective protections for maintaining privacy and fails to provide safeguards. With broad scope of exceptions, it has made the protections quite meaningless.

The law may deter technology and social media centered businesses from functioning smoothly in the country, since they will not be able to guarantee complete privacy to customers in Australia. Businesses will have to practice high level of caution to avoid any legal troubles concerning the digital rights of customers.

ABOUT THE AUTHOR

Pratham Arora is a Risk Intelligence Consultant at WoRisGo. He is currently an undergraduate at Ashoka University, studying Political Science, International Relations, and Philosophy. His primary areas of interest include diplomacy, international relations theory, and conflict analysis.