Communications Alliance
Responses to Questions on Notice
Public Hearing, 10 March 2021
PJCIS review into the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*

QoN 1:

Mr BYRNE: "[…] From your dealings with counterparts oversees, are you aware of whether the Metropolitan Police or the FBI have the power that the AFP and ACIC are seeking?"

Communications Alliance response:

We believe this question may be best answered by independent research, the Law Council or other stakeholders with greater international reach.

Our research indicates that the United States has a piece of legislation that grants some of the powers contemplated in the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* but those powers are significantly less intrusive than those proposed in the Bill.

Federal Rule of Criminal Procedure 41(b)(6) (enacted in 2016) allows law enforcement to remotely access a target computer/server. Rule 41(b)(6) allows Courts to issue search warrants authorising law enforcement to remotely hack into a target computer/server through spyware or malware and thus track its location and intercept data from it. These warrants, while controversial, have been largely upheld in the US Courts of Appeals. Rule 41(b)(6) is used mainly to collect intelligence on anonymous actors, similar to the network activity warrant.

However, Rule 41(b)(6) does not permit altering or deleting data from the target computer.

The Rule does also not authorise an "account takeover."

In addition, there is no corresponding requirement on service providers to assist law enforcement in these efforts.

QoN 2:

CHAIR: "[…] I'm specifically interested in the account turnover warrant. To give it a more specific example: a warrant is granted to take over the account of a WhatsApp user. On that WhatsApp user they have illegal content which is of interest to law enforcement but is also irrelevant content. I'm trying to understand what additional safeguards you're proposing to protect that irrelevant content or those innocent users that just happen to have a WhatsApp connection with that person, who is also engaging in unlawful behaviour?"

Communications Alliance response:

So far, we have not received any further suggestions from our members with regards to additional privacy protections that ought to apply in this scenario, beyond measures that would appear normal in all circumstances (safe and secure storage of the data etc.).