

Thursday, 11 March 2021

## Law Council questions need for broad surveillance powers

*All comments to be attributed to Law Council President, Dr Jacoba Brasch QC.*

“The Law Council of Australia appreciates the need for law enforcement agencies to have robust powers especially to counter cyber-enabled offences, such as serious and harmful crimes carried out online, like child exploitation and terrorism.

But if passed, the three new warrant-based powers proposed in the Surveillance Legislation Amendment (Identity and Disrupt) Bill 2020, will fundamentally alter Australia’s criminal intelligence framework, and potentially reach into and disrupt the lives of innocent bystanders.

In its current form, one of the warrants in the Bill would enable the Australian Federal Police (AFP) and/or the Australian Criminal Intelligence Commission (ACIC) to disrupt data that may be used in criminal activity with a maximum penalty of three or more years’ imprisonment.

An example of which may include enabling the disruption of entire computer networks, such as those used by people to organise activities or protests relating to pandemic lockdowns and which may breach public health directions.

These warrants can also be accompanied by compulsory assistance orders, which can require any person to provide information or assistance to the AFP or ACIC, with a potential penalty of 10 years’ imprisonment for non-compliance.

This is in direct conflict with a key recommendation of the Comprehensive Review of the Legal Framework of the National Intelligence Community (Richardson Review) released last year, which recommended that law enforcement agencies should not be given the specific cyber-disruption powers as proposed by this Bill.

The Law Council is concerned that a lack of evidence has been provided to show why the AFP and the ACIC require these powers. The breadth of the provisions also allows for the inadvertent capture of a wide range of benign conduct that could disrupt the lives of innocent bystanders.

The Richardson Review noted that there was a risk of mistakes being made in the targeting or execution (or both) of warrants, which may have disastrous and far-reaching consequences for third parties who are using, or are otherwise reliant on, services provided via a computer system or network, and are not under any suspicion of criminal wrongdoing.

Proposals to allow disruption offshore also creates a duplication of powers with the Australian Signals Directorate to disrupt cyber-enabled crime by persons or organisations outside Australia that could jeopardise the security and effectiveness of offshore disruption. It may also lead to inefficiencies in the use of public resources by multiple agencies in conducting substantially similar disruption operations outside Australia.

The Law Council believes that the Bill should be carefully scrutinised by the Parliament, particularly given the significant risks which arise from the doctrine of the rule of law and the separation of powers.”

**Contact:** Dr Fiona Wade, P. 0403 810 865 E. [Fiona.Wade@lawcouncil.asn.au](mailto:Fiona.Wade@lawcouncil.asn.au)