

Parliamentary Joint Committee on Intelligence and Security

Inquiry into the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

ANSWERS TO QUESTIONS ON NOTICE

Office of the Commonwealth Ombudsman

APRIL 2021

Department/Agency: Office of the Commonwealth Ombudsman

Question: 1

Topic: Independent process for technical expertise to be sought in issuing a warrant and consultation with communications service providers before a warrant is sought

Question:

Dr ALY: I have a follow up question along the lines of Mr Wilson's questions around technical capability. I don't know if any of the current witnesses were listening to the previous witness, who put in a suggestion that there would be some form of independent technical advice as a form of consultation in the execution of warrants. I was wondering if the current witnesses had any input into that recommendation that was made by the previous witness? ... No, it was the recommendation made by the previous witness, the Communications Alliance. They recommended an independent process by which technical expertise could be sought in the execution of a warrant, along with consultation of the platform providers.

Mr Manthorpe: I will also take it on notice, but I'm not aware that we have had any engagement with the Communications Alliance on the question. We will take it on notice to see if there is any more that we can contribute on this point. I would add that, if additional safeguards were put into the Bill – whether that happens is essentially a policy question – to address some of the sorts of concerns that are being raised then I would still maintain that we have the technical capability to ensure that the additional safeguards, if they are in the Bill, are adhered to. That would be our goal in designing the oversight approach.

Answer:

The Office of the Commonwealth Ombudsman is aware the Communications Alliance recommended the judicial authorisation process for the three proposed warrants should be informed by independent technical advice, and that the AFP and the ACIC should consult the designated communications provider before seeking a warrant.

We consider this is a policy decision for Government.

Question: 2

Topic: Nature of warrants overseen by the Commonwealth Ombudsman and whether they are different to a data disruption warrant

Question:

Senator KENEALLY: You made reference to other warrants that you oversight. Do any of them have this type of purpose similar in purpose to a data disruption warrant – that is, that they are not there to gather evidence, they're actually there to stop a crime being committed.

Mr Manthorpe: We might take that on notice, Senator Keneally. I'm happy for us to go away and think about whether we can add anything useful to respond to that.

Answer:

Most warrants and authorisations the Office oversees require either the person applying for the warrant/authorisation, or the issuing authority (Judge / AAT member / authorised officer) to be satisfied the warrant/authorisation is for the purpose of enabling evidence to be obtained, investigating an offence, or enforcing the criminal law.

However, warrants to monitor compliance with control orders are similar in nature to data disruption warrants, in that they are directed at preventing the commission of certain terrorist offences, or determining compliance with a control order.

To ensure compliance with a control order, the Australian Federal Police can obtain a telecommunications interception warrant, surveillance device warrant or tracking device authorisation to monitor compliance with the control order. When issuing such a warrant, the issuing authority must be satisfied, amongst other things, that the warrant is necessary to:

- protect the public from a terrorist act; or
- prevent support for, or facilitation of, a terrorist act; or
- prevent support for, or facilitation of, engagement in a hostile activity in a foreign country; or
- determine whether the control order, or any succeeding control order, has been, or is being, complied with.