COMMUNICATIONS ALLIANCE LTD
www.commsalliance.com.au

12 February 2021

Senator James Paterson
Chair
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600

Dear Senator Paterson,

RE: *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*

Communications Alliance welcomes the opportunity to make a submission to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) inquiry into the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (Bill).

Communications Alliance members comprise carriers and carriage services providers (C/CSPs) but also search engines and digital platforms. These two groups of communications service providers may be impacted quite differently by the proposed legislation.

Industry shares Government's desire to protect national security, fight terrorism and crime, enforce law and to enable the relevant agencies to do so effectively in a digital age. Member companies already provide law enforcement and intelligence agencies with various assistance, e.g. under the mandatory Data Retention Regime, the Telecommunications Sector Security Reform (TSSR) and/or through the workings of interception legislation and assistance obligations under the *Telecommunications Act 1997*. We also actively engaging with all stakeholders on the proposed Security of Critical Infrastructure Reforms currently underway and also before the PJCIS.

Consequently, our members support the intent of the Bill, but believe that some aspects of the Bill – for example around judicial authorisation, offence thresholds, consideration requirements etc. – require further work in order to meet the requisite tests of proportionality, effectiveness, practicality and feasibility.

While there may be further areas for comment, we will confine our feedback at this stage to some key areas of concern as they arise for members from an operational, compliance, security and/or risk management perspective. Please note that Communications Alliance members may make additional individual submissions.

1. Consultation with communications service providers

   The Bill proposes three new warrants for intelligence agencies, i.e. data disruption warrants, network activity warrants and account takeover warrants.

   A warrant of the kind described in the draft legislation has the potential for far-reaching consequences on the operations of a communications network/platform (and beyond!) which may – despite deep expert knowledge – not have been anticipated by the requesting agency.

   Consequently, we request that the Bill be amended to provide that the service provider who will be required to action a warrant, or assists with or facilitates its execution, ought

to be consulted prior to a warrant being issued. Doing so will not necessarily slow down the process but rather also confirm that the most appropriate provider has been approached, provide a means to streamline the process and/or ensure the most effective means to disrupt the targeted activity can be applied.

2. Authorisation of coercive powers:

The Bill proposes that, while account takeover warrants are to be issued by a magistrate, data disruption and network activity warrants can be issued by an eligible judge or a nominated member of the Australian Appeals Tribunal (AAT). Section 13 of the *Surveillance Devices Act 2004* (SD Act) stipulates that a nominated AAT member can include any member of the AAT, including full time and part-time senior members and general members. (Part-time senior members and general members can only be nominated if they have been enrolled as a legal practitioner for at least five years.)

As with the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act) and the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020*, and similar to the safeguard in the Bill of reserving the power to issue account takeover warrants to magistrates, we recommend that the Bill be amended to require independent judicial oversight and authorisation of data disruption and network activity warrants, given the potential intrusiveness of the warrants where they relate to interception, stored communications or communications data of individuals, i.e. covert access to potentially significant amounts of personal information.

We note that the Senate Standing Committee for the Scrutiny of Bills has equally highlighted this point in its recent *Scrutiny Digest 1/21, 29 January 2021*:

> *"The committee has had a long-standing preference that the power to issue warrants authorising the use of coercive or intrusive powers should only be conferred on judicial officers. In light of the extensive personal information that could be covertly accessed, copied, modified or deleted from an individual's computer or device, the committee would expect a detailed justification to be given as to the appropriateness of conferring such powers on AAT members, particularly part-time senior members and general members. In this instance, the explanatory memorandum provides no such justification."*[1]

It is noteworthy that the Senate Standing Committee made very similar comments for the two other pieces of legislation/draft legislation mentioned above.

3. Appropriate information and considerations prior to the issuing of warrants

As with previous pieces of legislation relating to national security, and against the background of our request for independent judicial authorisation, we believe that the judicial authorisation process ought to be informed by independent technical advice, e.g. on the intended method of disruption and the potential risks to networks, third parties or other 'collateral damage'. It is not hard to imagine that such damage may extend to damage of a whole network of devices which may include health care, emergency alert or even life support devices.

The Investigative Powers Commission approach suggested by the Independent National Security Legislation Monitor (INSLM) as part of his Report *TRUST BUT VERIFY A report concerning the Telecommunications and Other Legislation Amendment (Assistance and*

[1] Para 1.101, p.30, *Scrutiny Digest 1/21, 29 January 202,* Senate Standing Committee for the Scrutiny of Bills

Access) Act 2018 and related matters would also be an appropriate model to adopt for the far-reaching powers contemplated in this Bill.

Similarly, we recommend that the list of things that the eligible judges (or AAT members as currently proposed) must have regard to prior to issuing a warrant ought to be extended to include a placeholder for additional considerations currently not listed but considered relevant by the relevant judge (or AAT member). This would allow that person to have regard to expert opinion on subject matters that may not be covered by the other items in the list such as consideration of the effect of the warrant on communications networks/platform and potentially far-reaching damage and/or infringement of privacy of third parties (see also further item 6 below).

4. Threshold of offences

The Explanatory Memorandum notes that the new powers are required "to collect intelligence, conduct investigations, disrupt and prosecute the most serious of crimes, including child abuse and exploitation, terrorism, the sale of illicit drugs, human trafficking, identity theft and fraud, assassinations, and the distribution of weapons."[2]

However, the definition of 'relevant offence' in Section 6 of the SD Act, which is the relevant definition for the purposes of the new powers, includes a broad list of offences which are generally those that carry a maximum penalty of imprisonment for at least three years.

The Senate Standing Committee for the Scrutiny of Bills, in our view again correctly, observes that this includes

> *"[…] offences under Financial Transaction Reports Act 1988; Anti-Money Laundering and Counter-Terrorism Financing Act 2006; Fisheries Management Act 1991; and Torres Strait Fisheries Act 1984. In addition, the regulations may prescribe additional relevant offences. Similarly, the definition of 'serious Commonwealth offence' in section 15GE of the Crimes Act includes offences punishable by a maximum term of imprisonment of 3 years or more relating to, amongst other matters, tax evasion, currency violations, illegal gambling, bankruptcy and currency violations, forgery, misuse of a computer or electronic communications, or other matters prescribed by the regulations. Noting this broad range of offences, the committee considers that an explicit requirement to consider proportionality in relation to issuing each of the warrants is important to ensure that the significant coercive powers authorised under these warrants are only exercised where necessary and appropriate."*

We concur with the Senate Standing Committee's view and recommend that the threshold for the offence be raised to 'serious offence' in line with the offence threshold of the *Telecommunications (Interception and Access) Act 1979* and equally with the recommendations by the INSLM for the TOLA Act.

5. Criteria for applying for network activity warrants

As currently drafted, the threshold for applications for issue of a network activity warrant is significantly too low. Effectively, the only real requirement is that a network activity warrant has to be "relevant to the prevention, detection or frustration of one or more kinds of relevant offences" (see the new 27KK(1)(b)(ii)) – which could almost be anything, especially given the broad range of what can constitute a relevant offence.

[2] Para. 4, p. 2, *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* Explanatory Memorandum

We recommend that the threshold for this warrant be amended, as is the case for the data disruption warrant and the account takeover warrant, to include a reasonable suspicion that a (serious) offence has been or is likely to be committed.

6. Account takeover warrants and privacy of third-party data

Our members take the privacy of their customers very seriously and invest significant resources into safeguarding their customers' accounts data and privacy more generally. Consequently, we raise concerns with the potential invasion of privacy of third parties that are not the subject of an account takeover warrant. The relevant provisions of the Bill ought to include protections for information that is being accessed in the course of such action but is unrelated to the crime under investigation.

In this context, we also note with concern that proposed Sections 27KE(2)(e) and 27KP(2)(e) for the authorisation of network activity warrants, which can be equally damaging for the privacy of third parties, do not specifically require the judge or nominated AAT member to consider the privacy implications for third parties of accessing third party computers or communications in transit.

The eligible judge or nominated AAT member ought to be required to have regard to the privacy of any individual affected by any of the new warrants under consideration.

7. Assistance Orders

The proposed new Sections 64A and 64B of the amended SD Act would allow law enforcement agencies to compel specified persons to provide reasonable information and assistance to agencies aimed at the execution of a warrant. Therefore, it is possible that communications platform providers could be captured in the potential net of recipients of such assistance orders. However, such orders would be more appropriately directed at either the (business) user (first priority) of such platforms that holds or manages the account in relation to which access is sought or the platform provider corporation rather an individual employee or officer.

If, as a last resort, an assistance order is directed at an individual employee or officer (rather than the business user or the platform corporation), this may give rise to a conflict between the order and the employee's work responsibilities/terms of employment. It may also create difficult situations regarding the extent to which communications and approval within the employer organisation is prevented because of the legal constrains pertaining to protected information. The Bill should address these issues by requiring that the technology provider organisation be the target of technical assistance requests and, where an individual is compelled to provide assistance, by facilitating and paying for independent legal advice and to protect the employee from possible adverse consequences (both in terms of damages and employment) arising from compliance with the order.

We look forward to further engaging with the PJCIS and all relevant stakeholders on this important Bill.

Please contact [redacted] if you have any questions.

Yours sincerely,

[redacted]

John Stanton
Chief Executive Officer
Communications Alliance