INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

20 December 2024

Mr Jake Blight
Independent National Security Legislation Monitor

By email: INSLM@inslm.gov.au

RE: Issues Paper - Data Disruption, Network Activity and Account Takeover Warrants – Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act)

The Internet Association of Australia (**IAA**) thanks the Independent National Security Legislation Monitor (**INSLM**) for the opportunity to respond to the consultation on its *Issues Paper: Data Disruption, Network Activity and Account Takeover Warrants – Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act)* (**Issues Paper**).

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet Service Providers. This response is therefore primarily in representation of these members. In addition, as a not-for-profit association keenly interested in the public benefit of the Internet, we also submit our response to promote the public interest, particularly in respect of the Internet and Internet related issues.

PART 2: USE, ONGOING NECESSITY AND EFFECTIVENESS OF SLAID POWERS

ONGOING NECESSITY AND EFFECTIVENESS OF SLAID POWERS

What specific contribution has the use of SLAID powers made to responding to cyber dependent and cyber-enabled crimes?
Have issues arisen in practice that significantly affect the effectiveness of SLAID powers for the purpose that they were intended?

We are concerned that there is not enough reporting on the effectiveness of the use of the SLAID powers. Given the extremely invasive nature of the SLAID powers, we believe there should be more information on where these powers have been deemed to be not only necessary in the investigation of serious crimes but also the only or best measure available to the AFP and/or ACIC in addressing such crimes. In a similar vein, due to the lack of publicly available information, it is not clear that requests to extend certain powers, such as the extension of the duration of the NAW is justified. This need for increased depth of reporting will be expanded on throughout our response, and in particular, in response to Part 4 of the Issues Paper.

PART 3: SAFEGURDS

ISSUING WARRANTS

Who should issue SLAID warrants?
What, if any, independent technical advice should be available to issuing authorities?

In principle, we support the calls that have been made in previous consultations that only judicial officers, and not magistrates or ART members should be given authority to issue SLAID warrants. We believe this reflects the serious nature of the crimes that these powers should only be used in association with. However, we understand the practical limitations associated with such a requirement that must be balanced. In addition, we consider the issue of who should be allowed to issue SLAID warrants is further compounded when considering the lack of technical training provided to the existing issuing authorities, on top of the fact that judicial officers are not able to rely on the resources of the court when issuing warrants due to the constitutional principle o f the separation of powers.

On one hand, it would be overly resource intensive and burdensome on the court system if all SLAID warrants were to be issued only by judicial officers, and those of superior courts no less. We acknowledge that this would impede the serving of justice, both in terms of the serious crimes that that the SLAID powers are intending to address, as well as other cases that need to be heard at court that may be delayed by the additional pressure on judicial officers. However, on the other hand, the lack of resources made available to issuing authorities in respect of their issuing of SLAID warrants, including the lack of technical training is a great disservice to the justice system that casts doubt as to whether SLAID warrants are being appropriately issued.

We therefore support the recommendation made by the previous INSLM, Dr Renwick as set out in paragraphs 4.45 to 4.46 of the Issues Paper. We support the establishment of a separate 'Investigatory Power Division' comprising of judicial officers and senior and experienced members of the ART that are provided resources in relation to their issuing of warrants, including technical training. This could circumvent the issues relating to the constitutional principle of separation of powers, whilst also ensuring that those who are given authority to issue warrants are not only experienced, but properly resourced and funded to fulfil their duties in relation to the SLAID Act.

Should there be some sort of public interest monitor (PIM) available to review applications and assist independent issuing authorities?
Would it support the work of issuing authorities (or PIMs) to be provided with information about how SLAID powers are used in practice and the outcomes of thematic reviews or inspections by oversight bodies?

In addition, a separate division could be further supported by a public interest monitor. We believe the PIM would be an integral part of ensuring appropriate safeguards and oversight, as well as in assisting the issuing authorities with their functions.

Furthermore both the issuing authorities and Pim should be provided with as much information as possible or practicable about how the SLAID powers are being used, the effectiveness as well as any adverse consequences of such use, as well as the outcomes of reviews and inspections by oversight bodies such as the IGIS or the Commonwealth Ombudsman.

WHEN CAN A WARRANT OR AUTHORISATION BE ISSUED

What, if any, changes should be made to key definitions including 'relevant offence', 'criminal network of individuals' and 'computer'?

At this stage, we do not believe we have enough information to make concrete recommendations on whether these definitions should be amended. In general and on principle, we are concerned about the broad nature of these definitions that seem to capture more than what is purported or intended to be targeted by the SLAID powers, and therefore, the adverse privacy implications. However, we understand that there are complexities involved and the potential need to have broad definitions to ensure the utility of the powers.

Therefore, we believe it is important that the AFP and ACIC provide more information to demonstrate whether:

- these broad definitions have in fact been necessary to stop crimes of the *serious nature* that these invasive powers are purportedly trying to address;
- investigation of a less serious crime that is captured by the current definition has in fact contributed to the uncovering of more serious crimes; and
- other safeguards that currently exist have been sufficient in curtailing the impacts of these intrusive powers on the broader public and those not directly linked, or intentionally involved in serious criminal activity.

Having this information to understand the actual effectiveness of the powers under the SLAID Act is necessary to determine and justify that the status quo should be maintained, despite the adverse impacts these invasive powers have on the rights and freedoms of individuals, or whether amendments are necessary to ensure a more robust framework that also provide more stringent protections of privacy and individual liberties.

Do the current issuing criteria provide sufficient safeguards or are changes required? In particular, are additional protections required for LPP and similar privileges, journalists and the risk of a cyber operation introducing potential systemic vulnerabilities?

We strongly believe that there needs to be additional safeguards to reduce the risk of unintended adverse consequences of the use of the SLAID powers on telecommunications networks and Internet access. The legislation should expressly mandate:

- issuing authorities to consider the systematic vulnerabilities that may be introduced as a result of SLAID activity
- the AFP and ACIC to provide information in its warrant request, as far as is reasonably practicable, what risks may be posed to the relevant telecommunications network; and
- the AFP and ACIC to engage in consultation with the relevant industry entity about the implications of the SLAID activity, as far as is reasonably practicable.

Furthermore, this highlights another reason why issuing authorities should be given technical training, as well as the utility in the existence of a PIM. Such measures are likely to decrease the risk of SLAID warrants being issued without a greater consideration of the adverse technical and systematic implications associated with certain SLAID activities.

Are the approving officers and the criteria for (internal) granting and (external) approval of emergency authorisations appropriate?

Where issuing officers find that an emergency authorisation of a SLAID power was not appropriate, they should have powers to order the destruction of any information obtained via such use of the SLAID power. Furthermore, the relevant legislation should limit the use and sharing of any data that

were obtained under an emergency authorisation of a SLAID power that has since been deemed inappropriate.

Are the provisions relating to assistance orders appropriate or are additional safeguards and/or specificity required?

We are concerned that the current operation of assistance orders is not adequate to ensure appropriate safeguards or oversight and believe the following amendments should be introduced:

- legislation should not allow for individual staff members of an entity being named on an assistance order instead of the communications entity itself;
- harmonisation of the form of assistance orders and applications to ensure clarity and reasonableness of the assistance being sought
- express requirements being introduced so that issuing authority are made to consider the privacy impacts of an assistance order, as well as that such assistance requests are justified and proportionate.

LIFE CYCLE OF DATA

Should there be an express requirement that the retention, analysis, use or disclosure of information obtained under warrants be necessary and proportionate?
Are additional statutory protections required for special categories of data?

We support the introduction of an express requirement the retention, analysis, use or disclosure of data obtained under SLAID warrants must be necessary and proportionate. We believe the current 5 years retention period is too long and should be subject to review as soon as practicable following the first 5-year period of the SLAID powers coming into force. The review should investigate and assess the utility and proportionality of this period, with considerations of the adverse implications this retention period has had on the privacy and individual liberties of the public.

In addition, there should be further protections for special categories of data.

Are the current disclosure and secondary disclosure provisions appropriate?

We are concerned that the disclosures to State and Territory law enforcement agencies, as well as the ASIO, ASIS, ASD and AGO, and the internal use of the information received by these bodies are too broad. As it pertains to State and Territory law enforcement agencies' use of information that have been obtained under use of a SLAID power, this should be limited to crimes that meet the threshold of 'relevant offences' (or its equivalent). We believe it is also unclear what limitations exist to restrict to whom these bodies can then make secondary disclosures of the information obtained via the use of the SLAID powers. Thus, there needs to be a more thorough review and reporting of the privacy implications of these disclosure and secondary disclosure mechanisms.

Should there be specific statutory safeguards in relation to disclosures to foreign entities?

We understand that Australian law cannot impose legislative obligations on foreign entities to review and destroy information obtained under the use of the SLAID powers. However, we recommend external support mechanisms where disclosure of data to foreign countries involved. For example, we recommend that legislation that Australian agencies don't share information with foreign entities unless agreements or arrangements are in place with foreign entities that require such entities to:

- periodically review and destroy information to meet the principles of necessity, reasonableness and proportionality; and
- act in good faith and cooperate with Australian agencies in respect of auditing the entity's compliance with such review and destruction arrangements.

PART 4: OVERISGHT AND REPORTING

THE OMBUDSMAN AND IGIS

Is the division of functions between the IGIS and Ombudsman in relation to SLAID powers an efficient and effective way for inspection and other oversight safeguards to operate?
Does each oversight agency have sufficient powers and functions? In particular, should the Ombudsman have a broader oversight mandate to assess the 'propriety' of activities connected to SLAID powers?

We do not consider the current oversight regime to be sufficient, particularly in the case of the Ombudsman. Importantly, the Ombudsman should have powers and functions for a more in-depth review of the SLAID regime that takes into account the reasonableness, proportionality and necessity of SLAID powers, rather than being limited to assessing compliance with the existing legislation. Especially given that the SLAID Act was only recently introduced, there needs to be a more thorough consideration of the utility and effectiveness of the regime. Furthermore, it is not clear why the Ombudsman does not have oversight over the issuing and operation of NAWs.

REPORTING, RECORD KEEPING AND NOTIFICATION REQUIREMENTS

Are the current requirements about reporting to Ministers appropriate?

In general, we believe the reporting requirements that apply to the various types of the SLAID activities should be made consistent and overall, more robust. For example, it is not clear why activity in relation to ATW should not be under the same reporting requirements as the DDW and NAW.

In addition, it is not clear why it is necessary to only report on the activities associated with a SLAID warrant once the warrant has ceased to have effect. Especially as this relates to reporting to the Minister, and not the public which we understand may require more secrecy where the information relates to ongoing operations. It seems prudent to provide as much information as possible to ensure appropriate oversight over the use of the SLAID powers.

Are the current public reporting requirements about SLAID powers appropriate?

Overall, we believe that public reporting in relation to SLAID powers should be expanded to provide more qualitative information. In particular, there should be information provided on the actual arrests and prosecutions made as a result of the SLAID powers. We believe this to be best practice in terms of transparency and improving public trust as well as critical to ascertaining the reasonableness, effectiveness and proportionality of the SLAID Act, and therefore, to justify the invasive nature of these powers. Furthermore, as iterated above we believe that assistance orders should be mandated as part of public reporting requirements.

Are the current record keeping obligations and requirements about notifying IGIS and Ombudsman of certain matters effective for facilitating oversight?

The current record keeping obligations and requirements in respect of IGIS and the Ombudsman do not seem sufficient. We believe the requirements should be made more consistent in respect of the different types of SLAID powers, and more robust overall. Especially given the particularly invasive nature of the SLAID powers, ensuring adequate oversight is fundamental to ensure an appropriate balance and justification of infringing on the rights and freedoms of individuals for legitimate purposes.

For example, it seems very problematic that agencies are not required to retain information whether information obtained under a ATW has been destroyed which would obfuscate IGIS and

Ombudsman's oversight functions in ensuring agencies' compliance with the data retention requirements, and therefore pose greater risks to the data security and privacy of individuals.

Furthermore, it seems the type of information that must be notified to the IGIS and Ombudsman is lacking. In particular whether activity authorised under a SLAID warrant has caused material loss or damage seems to be exactly the type of information that the oversight bodies should have access to. Similarly, where agencies have breached the conditions of a warrant or otherwise failed to comply with relevant legislation is important information that is critical to the oversight functions of the Ombudsman and IGIS.

CONCLUSION

Once again, IAA appreciates the opportunity to contribute to the INSLM's review into the AFP and ACIC's powers under the SLAID Act. We look forward to engaging further with the INSLM, law enforcement and intelligence agencies, as well as other relevant stakeholders to ensure that the SLAID regime is fit for purpose and strikes an appropriate balance between combatting serious crime, upholding the rights and freedoms of individuals, as well as the impact on industry.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IX-Australia is a service provided by the Internet Association of Australia to Corporate and Affiliate members. It is the longest running carrier neutral Internet Exchange in Australia. Spanning six states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

IAA is also a licenced telecommunications carrier, and operates on a not-for-profit basis.

Yours faithfully,

Narelle Clark
Chief Executive Officer
Internet Association of Australia