Australian Information Industry Association

Australian Information Industry Association

Submission on

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

Introduction

The Australian Information Industry Association ('AIIA') appreciates the opportunity to provide feedback on the Issues Paper - Data Disruption, Network Activity and Account Takeover Powers – Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act).

This submission builds on the AIIA's 2021 input to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) review of the SLAID Bill. The AIIA has been a keen supporter of a safe Australian digital economy and understands the proposed need for the SLAID powers. Nonetheless, we note that in the three years since the Act came into force, there has been a total of 21 warrants issued but only one arrest made, according to Tables 1 and 2 of the Issues Paper. Even then, it is unclear if the one arrest resulted in a conviction. This submission highlights concerns and recommendations to ensure that the SLAID Act achieves its objectives proportionately, effectively, and with robust oversight.

Technical and Security-Related Factors for Decision-Makers

The current framework requires decision-makers to consider specific factors when assessing warrant applications, such as those outlined in *Crimes Act* s3ZZUP for Account Takeover Warrants. These include the gravity of the offences, the existence of alternative means, privacy impacts, evidentiary value, and previous warrants sought or issued in connection with the same alleged offence. While these factors provide important safeguards, they do not address the critical technical and security-related implications of the requested actions.

The AIIA recommends that the government include technical feasibility and security implications as part of the warrant approval process. This includes ensuring that applications demonstrate the practical viability of the requested actions and address potential risks to system security. Sections such as 33ZZUP should list relevant factors informed by a holistic awareness of the systems involved.

Independent Technical Advice

The AIIA recommends the integration of independent technical advice into the decision-making processes for the issuance of warrants. The complex and highly technical nature of the warrants introduced by the SLAID Act requires decision-makers to have access to expertise that ensures actions are both operationally feasible and proportionate. The current proposal outlined in chapter 4 of the Issues Paper, to grant issuing authorities, such as judicial officers and tribunal members, access to independent technical advice during the warrant approval process is a positive step. However, the AIIA believes that incorporating independent advice earlier in the process, during the application stage, would provide significant additional benefits. For example, we note that the possible misuse of emerging technologies such as Artificial Intelligence (AI)/deepfake technologies could be mistaken for actual child abuse material, leading to misplaced efforts.

The disparity between the number of warrants issued and arrests made raises questions about the effectiveness of the current warrant application process. Independent advice could address potential gaps in feasibility assessments and evidentiary sufficiency, preventing the misuse of resources on actions unlikely to yield meaningful outcomes. The AIIA suggests that the government stand up an independent board or approved list of communications and technology technical experts that are consulted before applications for warrants are made. This board would have regard to security, integrity and technical feasibility considerations of government intervention in systems and networks and could provide advice to both government and industry in facilitating the disruption of crime in a reasonable, proportionate and technically feasible fashion.

Cost Recovery Provisions

The absence of cost recovery provisions could place an undue financial strain on private entities, particularly in cases involving complex or resource-intensive compliance requirements. This risk is amplified for smaller entities, which may lack the internal capacity to handle such demands without significant disruption to their operations.

The AIIA suggests that the legislation provide for cost recovery for private entities for the costs that they incur in implementing assistance orders. This provision would be enlivened where there is a significant loss or extraordinary cost to the assisting entity, whether in repairing vulnerabilities, restoring service, addressing a human resources burden, or intensive technical impact incurred by the company in complying with an assistance order.

Clarification of Roles and Responsibilities of 'Specified Persons'

The AIIA seeks further clarification of the roles and responsibilities of a 'specified person' in the legislation (*Surveillance Devices Act* ss 64A and 64B(1), *Crimes Act* s 3ZZVG), and what 'provid[ing] any information or assistance that is reasonable and necessary' could constitute in the context of what law enforcement could compel a 'specified person' to do.

This ambiguity raises concerns about the scope and limits of their obligations, as well as the potential for overreach or inconsistent enforcement.

Mandatory Consultation Clause

The execution of warrants under the SLAID Act can impose substantial technical, operational, and legal burdens on affected entities. Despite this, the current legislation does not require law enforcement to consult with these entities before applying for or executing a warrant. This lack of engagement increases the risk of technical complications, operational disruptions, and inefficiencies that could otherwise be mitigated through early consultation.

While it is acknowledged that consultation may not always be feasible—particularly in covert police operations where time constraints or confidentiality concerns preclude engagement—there remains a significant opportunity to strengthen the decision-making process. Requiring issuing authorities to assess whether consultation has occurred, and, if

not, whether its absence is reasonable in the circumstances, would provide a balanced approach. This ensures that consultation is encouraged where it can add value, without compromising the objectives of sensitive operations.

When consultation is appropriate, it should involve a formal and confidential process that notifies the affected entity or network of the pending warrant. This notification should include an outline of the reasons for the warrant application and a description of the assistance required. Such engagement would allow the entity to evaluate the technical feasibility of the proposed actions and assess the potential operational impacts. By being involved early, the entity can contribute to the warrant's practical design, ensuring a smoother and more efficient execution while maintaining the integrity of the investigation. Similar provisions have been codified in other statutory schemes, such as the *Telecommunications Act*.[1]

Raising the threshold for eligible offences and 'reasonable suspicion'

The current threshold for issuing warrants relies on 'reasonable suspicion' of the commission of an offence. While this standard is a recognised legal threshold, it allows for action based on limited or circumstantial evidence. Given the intrusiveness of the powers authorised under the SLAID framework, a higher standard of evidence is warranted to ensure the proportionality and appropriateness of these measures. The AIIA recommends raising the threshold to 'reasonably believing on the grounds of probative evidence.'

In addition, the three-year offence issuing threshold creates the potential for overreach, allowing for warrants to be issued for offences that fall outside the scope of the serious and high-impact crimes that the framework seeks to address.[2] The AIIA recommends that the threshold be increased to offences punishable by at least seven years' imprisonment or those that have a demonstrable impact on public safety, national security, or critical infrastructure.

Reconsidering the seriousness of the penalty regime

The penalties under the SLAID framework include significant consequences for non-compliance with assistance orders or for actions such as unauthorised disclosure of warrant information. The AIIA cautions that the imposition of overly stringent penalties—up to 10 years' imprisonment or 600 penalty units—is disproportionate, particularly in the absence of appropriate good faith immunity provisions.

Publishing or communicating warrant information–where such publication or communication is considered to prejudice the effective conduct of an investigation–or

[1] *Telecommunications Act 1997* (Cth) ss 317PA(1), 317W(1).
[2] *Revised Explanatory Memorandum*, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) ss4, 25, 41, 45.

being deemed uncooperative with warrants despite one's ability to cooperate, are some of the offences that would incur such penalties.

The AIIA submits that these penalties are disproportionate, especially where they could be applied to officers, employees or agents of entities on the matter of interpretation of their conduct, or where their conduct is well-intentioned or inadvertent, as opposed to the criminal actor themselves.

Limit issuing authority to judicial officers

The AIIA calls on the government to only allow the issue of warrants by judicial officers, not members of the Administrative Review Tribunal (ART). While the AIIA respects the ART and its remit, the extraordinary powers of intervention and hacking allowed for by these new warrants calls for a high judicial threshold where the rule of law and jurisdictional implications are carefully considered by an experienced and senior member of the judiciary. Due to the handful of applications each year according to Tables 1 and 2, this is likely a manageable responsibility for judicial officers.

Emergency Authorisations and controls on data gathered

The AIIA is concerned with the emergency authorisation powers as well as the inadequate controls such as the lack of specific statutory controls or safeguards to protect privacy or other rights in the course of the analysis of data gathered under SLAID warrants or the lack of express legislative requirement to consider necessity, proportionality or impact on privacy or other rights when making an authorised disclosure. For this reason, we are keen to see reports from either the Ombudsman or IGIS and Public Interest Monitors on the impact on Australians' civil liberties.

Allow merits review of decision to grant warrant

Currently, there is no mechanism to seek a substantive reassessment of the grounds upon which a warrant has been granted. This absence of merits review restricts the ability of affected entities to challenge whether the warrant is justified, proportionate, or supported by sufficient evidence. The AIIA recommends that affected entities should be able to appeal from the order to grant a warrant where they believe the issuance was inappropriate, with proper merits review processes in place for another judicial officer to reconsider the decision.

Conclusion

The AIIA appreciates the opportunity to contribute to the review of the SLAID Act and acknowledges the critical role these powers play in combating serious and cyber-enabled crimes. However, the intrusive nature of these powers necessitates robust safeguards, clear accountability mechanisms, and proportional applications to maintain public trust and industry cooperation.

By incorporating the recommendations outlined in this submission, the SLAID framework can be strengthened to better balance effective law enforcement with the protection of rights and operational integrity.

Should you require further information, please contact Ms Siew Lee Seow, General Manager, Policy and Media, at siewlee@aiia.com.au or 0435 620 406, or Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Thank you for considering our submission.

Yours sincerely
Simon Bush
CEO, AIIA

***

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies