THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: CLC/PuLC/PDL:BMml061224

6 December 2024

Dr James Popple
Chief Executive Officer
Law Council of Australia
PO Box 5350
Braddon ACT 2612

By email: Shounok.Chatterjee@lawcouncil.au

Dear Dr Popple,

**Review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021***

Thank you for the opportunity to contribute to the Law Council's submission in response to the review by the Independent National Security Legislation Monitor (**INSLM)** of amendments made by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (**SLAID Act**) to the *Surveillance Devices Act 2004* (Cth) and the *Crimes Act 1914* (Cth). The Law Society's Criminal Law, Public Law, and Privacy and Data Law Committees contributed to this submission.

**Arrangements for issuing warrants**

In our view, given the potential reach of data disruption warrants (**DDWs**) and network activity warrants (**NAWs**), it would be preferable for the issuing authority to be eligible superior court judges rather than, as presently occurs, extending to members of the Administrative Review Tribunal (**ART**). We support the views previously expressed by the Law Council in its submission on the Bill which noted the greater skill and experience of superior court judges compared with ART members, and the need for public confidence in the issuing process.

If eligible judges of superior courts lack the necessary technical knowledge in relation to surveillance powers, training should be provided. While the Issues Paper suggests that practical considerations, including technical complexity, may stand in the way of providing such training, we consider that in order to make an informed decision, any person issuing a warrant should be aware of the capabilities and risks of the relevant surveillance method.

**Issuing warrants**

In our view, the definition of "criminal network" is overly broad. The definition includes use of a "service", but there is no limit to what a "service" is, nor any requirement that a person using the service be in any way connected to the criminal activity. This has been identified previously as an issue.[1] We support the recommendation for the definition to be amended to require a reasonable suspicion of a connection between the suspected conduct of the individual group

[1] See Law Council submission to the Parliamentary Joint Committee on Intelligence and Security, *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*, 9 March 2021, online: https://lawcouncil.au/publicassets/c7feaa1c-bb80-eb11-943a-005056be13b5/Surveillance%20Legislation%20Amendment%20%20Identify%20and%20Disrupt%20%20Bill%202020.pdf.

member in committing an offence or facilitating the commission of an offence; and the actions or intentions of the group as a whole.[2]

Similarly, an "account" (for the purpose of a NAW) is effectively unlimited. Given that online or subscription access is now the norm for almost all services (including services which are otherwise unrelated to anything electronic or cyber-related), this would seem to extend search warrant powers enormously.

Each warrant allows for the access to and changing of data beyond the specific target of the warrant if "necessary" for the purpose of the warrant. This expands the potential impacts, without the oversight of the decision maker on the warrant. In our view, there is potential for misuse or scope creep in the absence of effective oversight.

The issue of scope creep also arises due to the presumption that any data "subject to a form of electronic protection" is "taken to be relevant for the purposes of determining whether the relevant data is covered by the warrant". "Electronic protection" does not seem to be defined.[3] Almost all electronic data is likely to be subject to some form of "electronic protection" – be that a password to access the computer, a firewall to protect against malware, data encryption (which is largely standard in many forms of communication) and data storage, particularly those used commercially. We query whether this means that almost any data accessed will be deemed relevant and captured by the warrant.

Notably, this could reduce the usefulness of the reporting. If all data accessed can be deemed relevant, then simply reporting that the data was collected in accordance with the warrant does not provide helpful information about whether the access was in fact necessary and proportionate.

**Privacy**

In our view, there appears to be limited acknowledgement of the privacy implications of these powers. There is no express protection for information that might be particularly sensitive (including legally privileged information, sensitive personal or medical information, and similar).[4] The Issues Paper acknowledges that many modern warrant thresholds, and the capabilities used to execute the warrants, potentially enable the collection of a great deal of data. This includes data about people who are not reasonably suspected of engaging in unlawful activity in order to identify and locate those who are.[5]

While there is a requirement to consider privacy "to the extent known" at the time warrants are issued, the weight to be given to that consideration is up to the decision maker – the judicial officer or ART member. We suggest that this risks limiting oversight and potential inconsistency in the way decision-makers give weight to privacy considerations. In our view, given the breadth of the powers, the fact that broad categories of information can be copied and shared, with the potential impact on persons who are entirely unrelated to the alleged criminal activity, creates significant risk that privacy will be given insufficient protection.

There appears to be no requirement to report explicitly on the extent to which information accessed did in fact result in access to, or disruption of, personal information of persons lawfully using the service/computer. It may be possible to draw inferences from the reported

---

[2] Recommendation 30, Parliamentary Joint Committee on Intelligence and Security, *SLAID Report* (2021) 146.
[3] Sections 27KE and 27KP of the SLAID Act.
[4] Independent National Security Legislation Monitor, *Issues Paper: Data disruption, network activity and account takeover warrants in the Crimes Act 1914 and Surveillance Devices Act 2004* (2024) 41.
[5] Ibid 47.

information. We believe that where there is no obligation to inform a person that their data or accounts have been accessed or altered, that information should not be left to inference.

Further, there appears to be no mechanism to inform people whose data has been accessed or modified. While we understand the possible rationale in the context of crime or crime prevention, it does mean that there is little avenue for individuals to seek redress for any overreach or wrongdoing. We believe the proposed public interest monitor, similar to the NSW Surveillance Devices Commissioner,[6] might mitigate this.

We consider further assessment of privacy impacts should be undertaken at later points when the full impact of privacy and other rights infringements are more fully realised following analysis of the data. A key issue is that the assessments of impact are generally focussed on substantive impacts or on "loss". However, access to information and accounts can be low "impact" in a tangible sense, while still having serious impacts on privacy.

In terms of authorised disclosure, we support an express requirement for the decision-maker to consider the necessity, proportionality or impact on privacy or other rights of making a disclosure, which is currently absent from the legislation.[7]

There is also no requirement to consider matters such as legal professional privilege, journalist privilege (except in limited circumstances) or other public interest considerations.[8] This may fall within the general considerations – however, again, given the breadth of the potential impact, we suggest this should be made explicit.

We note, as the Issues Paper also acknowledges, that many of these issues have been previously identified in response to the earlier inquiry by the Parliamentary Joint Committee on Intelligence and Security into the Bill, and many recommendations were not implemented when the legislation was passed. However, we believe that these issues remain significant in an increasingly digital world. There is little prospective protection, and reporting after the fact may not be sufficiently informative to guarantee effective oversight. We believe a public interest monitor might assist to mitigate some of the risks identified.

Thank you for the opportunity to contribute to the Law Council's submission. Questions at first instance may be directed to Mimi Lee, Policy Lawyer, at (02) 9926 0174 or Mimi.Lee@lawsociety.com.au.

Yours sincerely,

Brett McGrath
**President**

[6] Independent National Security Legislation Monitor, *Issues Paper: Data disruption, network activity and account takeover warrants in the Crimes Act 1914 and Surveillance Devices Act 2004* (2024), 29.
[7] Ibid, 50.
[8] Ibid, 41.