

WE NEED TO MODERNISE THE SYSTEM FOR ISSUING WARRANTS: KEY FINDINGS FROM THE INDEPENDENT REVIEW OF THE *SURVEILLANCE LEGISLATION AMENDMENT (IDENTIFY AND DISRUPT) ACT 2021* (CTH)

JAKE BLIGHT*

Cyber-enabled and cyber-dependent crime is a growing problem. One legislative response was the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) which gave the Australian Federal Police and the Australian Criminal Intelligence Commission access to three new warrants. The warrants go well beyond traditional surveillance powers and enable the collection of data on a large number of people, the takeover of online accounts, and the active alteration of data online. The warrants have been useful, but their potential to infringe privacy and other rights is significant. This article, written by the Independent National Security Legislation Monitor, explains why the current safeguards are inadequate and how the system for issuing warrants and related provisions need reform. These findings have implications for a range of other electronic surveillance powers. The article also provides insight into how tools from systems theory were used to inform the process and findings of the Monitor's review.

I INTRODUCTION

The Independent National Security Legislation Monitor ('INSLM') is a statutory officer charged with examining the necessity, proportionality and effectiveness of national security and counter-terrorism laws. Such reviews must also have regard to Australia's international obligations, including human rights obligations.¹ In effect, the INSLM and their staff are a specialist law reform body and part of the broader oversight architecture for security, intelligence and police powers. The author of this article is the current Monitor, having been appointed in September 2023 for a three-year term.²

* Jake Blight is the Independent National Security Legislation Monitor. He was formerly an Associate Professor at the Australian National University, National Security College.

1 *Independent National Security Legislation Monitor Act 2010* (Cth) ss 6, 8 ('INSLM Act').

2 Mark Dreyfus, 'Appointment of the Independent National Security Legislation Monitor' (Media Release, Attorney-General, 14 September 2023) <<https://webarchive.nla.gov.au/awa/20230921094409/https://ministers.ag.gov.au/media-centre/appointment-independent-national-security-legislation-monitor-14-09-2023>>.

One of the reviews I have undertaken as Monitor is a review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) ('*SLAID Act*'). The report of this review was tabled in Parliament in September 2025.³ I found that the special powers in the *SLAID Act* were needed and should largely be retained, with one major caveat. That caveat concerned the system for issuing warrants.⁴ The report explains that I consider the main safeguard for the granting of these powers, the current system for issuing warrants, to be inadequate for powers authorising the use of advanced technical capabilities, collection of bulk data or disruption, particularly when they can be exercised covertly.⁵ This finding has implications beyond the *SLAID Act* warrants. Firstly, because it re-frames the idea of issuing warrants as a 'system' rather than an action; and secondly, because the deficiencies identified in the current system are present in other warrants, including those currently being examined in the long-running government electronic surveillance reform project.⁶ The changes that I have recommended to the system for issuing warrants are a significant departure from the status quo. They include moving away from the use of Administrative Review Tribunal ('ART') members to issue warrants in favour of retired judges, introduction of public interest monitors, access to independent technical advice and an independent system for allocating warrants to decision makers.⁷ It is thus not entirely surprising that the Government

3 Jake Blight, Independent National Security Legislation Monitor, *Data Disruption, Network Activity and Account Takeover Powers: Review of Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Report, 31 July 2025) <<https://www.inslm.gov.au/publications/data-disruption-network-activity-and-account-takeover-powers-review-surveillance-legislation-amendment-identify-and-disrupt-act-2021>> ('*INSLM SLAID Act Report*').

4 Recommendations 1–3 relate to the retention of data disruption, network activity and account takeover warrants respectively. Each recommendation expressly states that retention is 'subject to recommendations 6–8'. Recommendations 6–8 set out the key elements of a proposed new system for issuing warrants: Department of Home Affairs, 'Australian Government Response to the Independent National Security Legislation Monitor: Review of the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*' (Government Document, November 2025) <https://www.aph.gov.au/Parliamentary_Business/Tabled_Documents/14422> ('Government Response to the *SLAID Report*'). The 'Government Response to the *SLAID Report*' said that it 'agreed' with Recommendations 1–3: at 2–3; though in the detail of the response, says that it will extend the sunset date for the powers 'in the first instance, in order to allow Recommendations 6–8 to be further considered' as part of its ongoing electronic surveillance review: at 2.

5 *INSLM SLAID Act Report* (n 3) i.

6 The electronic surveillance reform project was recommended in Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Report, December 2019) vol 2, 266–8 ('*2019 Comprehensive Review*'). The project commenced in 2020 and was initially conceived of as a two-year project with a Bill to be finalised in 2023: 'Electronic Surveillance Reform', *Department of Home Affairs* (Web Page, 6 December 2021) <<https://webarchive.nla.gov.au/awa/20220328194515/https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/electronic-surveillance-reform>>. Responsibility for the project has since been moved from the Department of Home Affairs to the Attorney-General's Department and then back to the Department of Home Affairs in a machinery of government changes. The Department of Home Affairs website currently refers to the project as 'a significant long-term undertaking': 'Reform of Australia's Electronic Surveillance Framework', *Department of Home Affairs* (Web Page, 18 July 2025) <<https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/electronic-surveillance/reform-of-australias-electronic-surveillance-framework>>.

7 Recommendations 6–9 of the *INSLM SLAID Act Report* (n 3).

response to most of the main recommendations, tabled on 10 February 2026, was to say that they would be further considered as part of its ongoing electronic surveillance reform project ‘as these recommendations are applicable to the electronic surveillance framework as a whole’.⁸

Changes in technology, as well as changes in law, mean that the scale at which privacy rights can be infringed through the exercise of surveillance and related powers has increased dramatically in the last 20 or so years, and *SLAID Act* warrants are emblematic of this.⁹ Preventing, disrupting and prosecuting serious crime is a legitimate objective for which necessary and proportionate infringement of privacy rights is permissible.¹⁰ Ensuring that our surveillance and related laws are appropriately tailored in their scope and have sufficient safeguards is essential to ensure compliance with Australia’s obligations under the *International Covenant on Civil and Political Rights* (‘ICCPR’).¹¹ Effective safeguards are also essential for maintaining public trust in the exercise of rights-invasive powers by police and intelligence agencies.

This article begins with an overview of the *SLAID Act* powers and why they were enacted. This provides context for the analysis of the system for issuing warrants. Of particular relevance is the potential technical complexity of the capabilities used to exercise some warrant powers and the significant volumes of data that can be obtained, retained and disseminated in reliance on *SLAID Act* powers. Part III of this article explains how I used aspects of systems theory to inform my thinking in the review and why I found this useful. Part IV provides information about my key recommendations and how these are informed by the idea of seeing the issuing of warrants as a ‘system’ rather than an ‘action’. Part V briefly explores potential broader implications of my findings on *SLAID Act* warrants, including what they may mean for wider electronic surveillance reform. The Government’s response to my report is discussed in relation to relevant recommendations and the ongoing electronic surveillance reform project.

II *SLAID ACT* POWERS

The need for the introduction of the *SLAID Act* powers was framed by reference to the growing threat of ‘serious crimes perpetrated using anonymising technologies

8 ‘Government Response to the *SLAID Report*’ (n 4) 1:

In response to the Monitor’s 21 recommendations, the Government has agreed to 4 of those recommendations, agreed 2 recommendations in part, and noted the remaining 15. The Government will further consider the recommendations that have been agreed in part or noted, as part of electronic surveillance reform, as these recommendations are applicable to the electronic surveillance framework as a whole.

9 *INSLM SLAID Act Report* (n 3) 13 [2.28].

10 Human Rights Committee, *General Comment No 16: Article 17*, UN Doc HRI/GEN/1/rev.6 (8 April 1988) 142 [4].

11 *International Covenant on Civil and Political Rights*, opened for signature 19 December 1966, 999 UNTS 171 (entered into force 23 March 1976).

and the dark web¹² and, more broadly, by the notion of ‘cybercrime’.¹³ Cybercrime is a term that encompasses both cyber-dependent and cyber-enabled crimes.¹⁴ Cyber-dependent crimes are crimes that did not exist before the proliferation of computers and information technology.¹⁵ This includes crimes relating to unlawful access and disruption of data on computers or networks of computers.¹⁶ Cyber-enabled crimes are other crimes that are enabled by computers and information technology such as drug smuggling and money laundering. Regardless of the exact distinction, crimes that are conducted or enabled through the use of increasingly advanced technology pose real challenges for police and criminal intelligence agencies.¹⁷

Encryption and other security hardening features of modern communications mean that traditional law enforcement capabilities and techniques are not well adapted to the challenges of gathering evidence and intelligence about cybercrime. For example, over 95% of the content received by the Australian Federal Police (‘AFP’) from traditional telecommunications interception is now unintelligible due to encryption.¹⁸ Crimes committed online can occur almost instantly and at an unprecedented scale. Consider, for example, how rapidly malware can spread and how many devices can be ‘infected’ or how broadly and quickly abhorrent or violent material can be shared online.¹⁹

It was these kinds of challenges that were cited to describe the need for the new legal powers contained in the *SLAID Act*.²⁰ The *SLAID Act* powers were never going to be a complete solution to the policing and law enforcement challenges of cybercrime. For example, more recent legislative changes made by the *Telecommunications and Other Legislation Amendment Act 2025* (Cth) were in part directed at police powers for combatting online child abuse.²¹ A current inquiry by the Parliamentary Joint Committee on Law Enforcement is considering

12 Commonwealth, *Parliamentary Debates*, House of Representatives, 3 December 2020, 10431–3 (Peter Dutton, Minister for Home Affairs).

13 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 31–2 [70], 42 [133], 97 [485], 180–1 [1047].

14 Australian Government, *National Plan to Combat Cybercrime 2022* (Report, 2022) 4 <<https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf>>.

15 *INSLM SLAID Act Report* (n 3) 14 [3.2]–[3.4].

16 Australian Federal Police, Submission No 22 to Parliamentary Joint Committee on Law Enforcement, Parliament of Australia, *Inquiry into the Capability of Law Enforcement to Respond to Cybercrime* (January 2024) 3 [15] <<https://www.aph.gov.au/DocumentStore.ashx?id=e3d5cb01-38ea-4099-a4eb-c7fff19f0a88&subId=752009>>.

17 *INSLM SLAID Act Report* (n 3) 17–18 [3.11]–[3.17].

18 Australian Federal Police, Submission No 18 to Independent National Security Legislation Monitor, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (10 January 2025) 3 [15] <<https://www.inslm.gov.au/system/files/2025-01/submission-18-australian-federal-police.pdf>> (‘AFP Submission’).

19 Australian Signals Directorate, *Annual Cyber Threat Report 2024–25* (Report, 14 October 2025) 19, 25 (‘2024–25 Annual Cyber Threat Report’); Explanatory Memorandum, Criminal Code Amendment (Sharing of Abhorrent Violent Material) Bill 2019 (Cth) 15–6 [20], 16 [23], 19–20 [40].

20 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth).

21 *Telecommunications and Other Legislation Amendment Act 2025* (Cth) sch 5 (‘TOLA Act’). See also Explanatory Memorandum, Telecommunications and Other Legislation Amendment Bill 2025 (Cth) 27.

the capability of law enforcement to respond to cybercrime.²² No doubt more powers, or changes to enhance powers, will be proposed in future.

In the course of my inquiry into the *SLAID Act* powers, I sought and received extensive evidence, both classified and unclassified, on how the powers had been used.²³ Ultimately, I was satisfied that the *SLAID Act* powers have been ‘effective in understanding criminal networks and combating serious crimes’ and that ‘they have been used in situations where other types of warrants would probably have been ineffective’.²⁴ Serious crimes committed or enabled online can, like other serious crimes, cause real harm to individuals and it is not controversial that preventing and disrupting such crimes is a legitimate objective of government. The key question is whether the *SLAID Act* powers are appropriately adapted and targeted to this objective and if the safeguards are sufficient. Assessing this requires an understanding of what the powers can authorise.

A Three New Warrant Types and Related Powers

The *SLAID Act* introduced three new types of warrants and associated emergency authorisations and assistance orders. The powers were described as ‘world-leading and novel’ when introduced.²⁵ This is an apt description. There remain few similar powers in comparable countries and, as described below, the powers diverge significantly from traditional police and criminal intelligence powers.

1 Network Activity Warrants

Network Activity Warrants (‘NAWs’) allow access to data in multiple computers about multiple people. Unlike most surveillance warrants, it is not necessary to identify the individuals to be surveilled in an application, nor the specific computers, nor is it necessary for police to have a reasonable belief that all of those under surveillance are suspected of involvement in criminal activity.²⁶

22 The inquiry into the capability of law enforcement to respond to cybercrime was initiated on 16 October 2023, lapsed at the end of the 47th Parliament and was re-referred by the committee of the 48th Parliament: ‘Capability of Law Enforcement to Respond to Cybercrime’, *Parliament of Australia* (Web Page) <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/LECybercrime47>.

23 This evidence is discussed in chapter 4 of the report: *INSLM SLAID Act Report* (n 3) 19–29. Copies of open submissions, transcripts of the public hearings as well as summaries of closed hearings are all available on the INSLM website: ‘Independent National Security Legislation Monitor’, *INSLM* (Web Page) <<https://www.inslm.gov.au>>.

24 *INSLM SLAID Act Report* (n 3) 29 [4.36].

25 Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory Report on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (Report, August 2021) 119 [6.1].

26 For example, to issue a service warrant in relation to a service used by a person under the *Telecommunications (Interception and Access) Act 1979* (Cth) (‘*TIA Act*’), the issuing authority needs to be satisfied that there are reasonable grounds to believe a particular person is using the service, and the proposed interception relates to investigation of a serious offence in which the particular person is involved: at ss 46(1)(c), (d)(i).

Instead, the ‘targets’ of surveillance are any computers²⁷ used by a ‘criminal network of individuals’ (a description I found to be misleading).²⁸ A criminal network of individuals is a group of ‘electronically linked individuals’ using the same electronic service where the service enables at least one individual in the group to engage in or communicate about a relevant offence; or to facilitate or communicate about facilitating another person (whether in the group or not) engaging in a relevant offence.²⁹ Examples of ‘electronically linked individuals’ given in the explanatory materials included all users of WhatsApp or Telegram.³⁰ According to WhatsApp, more than 3 billion people in over 180 countries use the WhatsApp messaging platform.³¹ An application for such a broad warrant would not be practical or in any way necessary or proportionate. The evidence was that warrants have been used judiciously.³²

Nevertheless, these warrants are powerful and are clearly intended to enable the collection of large amounts of data about many people. That data can then be retained, analysed and shared with other agencies, including Australia’s security and foreign intelligence agencies and their overseas partners.³³ NAWs do not have the usual ‘reasonable suspicion of involvement in criminal activity’ test as part of their issuing criteria, rather the threshold for the AFP or the Australian Criminal Intelligence Commission (‘ACIC’) applying for a warrant is a reasonable belief that the warrant will ‘substantially assist’ in the collection of *intelligence* about the network and which is ‘*relevant* to’ prevention, detection or frustration of one or more relevant offences.³⁴ Clearly, this is a much lower threshold.

NAWs are intended to be used as an intelligence tool rather than a traditional evidence-gathering mechanism.³⁵ This is evident from the fact that NAW material is inadmissible as evidence in most criminal proceedings.³⁶ This is a sound protection. But a consequence of it is that individuals whose data has been collected under a NAW are extremely unlikely to ever know this has occurred; thus, they are extremely unlikely to have the opportunity to challenge the validity of the warrant.

27 The word ‘computer’ is defined as including multiple computers, computer systems and computer networks: *Crimes Act 1914* (Cth) s 3ZZUK (‘*Crimes Act*’); *Surveillance Devices Act 2004* (Cth) s 6 (‘*SD Act*’).

28 Recommendation 10 of the *INSLM SLAID Act Report* (n 3) 9 [2.13], 139–40 [10.44]–[10.47].

29 *SD Act* (n 27) s 7A.

30 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 80–1 [398]–[399].

31 ‘About WhatsApp’, *WhatsApp* (Web Page) <<https://www.whatsapp.com/about>>.

32 *INSLM SLAID Act Report* (n 3) 24 [4.12]–[4.14].

33 See *SD Act* (n 27) ss 45(4)(c)–(d), 45B(4)(d)–(e); *ibid* 169 [12.16].

34 *SD Act* (n 27) s 27KK(1) (emphasis added).

35 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 4–5 [17]–[19]. See also the example provided by ACIC of how material gathered under NAWs has contributed to intelligence about individuals who have been arrested, but that as arrests are strictly based on admissible evidence, the material gathered under the NAW is not described as leading to the arrest: *INSLM SLAID Act Report* (n 3) 26 [4.25].

36 *SD Act* (n 27) ss 45B(1), (3), (10).

I received evidence that NAWs have been used by both the AFP and ACIC to obtain intelligence relevant to criminal activity.³⁷ During a public hearing, ACIC gave evidence that they have used these warrants to identify a criminal syndicate not previously known to be operating in Australia, something that they may not have been able to identify, or at least not as early or easily, without the use of NAWs.³⁸

2 Data Disruption Warrants

Data Disruption Warrants ('DDWs') are the most unusual of the three *SLAID Act* warrants. They are not a surveillance warrant, rather they authorise the addition, copying, deletion or alteration of data in order to 'frustrate' a crime.³⁹ Such activity is otherwise itself a serious crime.⁴⁰ There is no requirement for any judicial finding that a crime has occurred or is likely to occur, either to the criminal or civil standard before a disruption warrant is issued.⁴¹ Nor is it likely that the use of a DDW will lead to later prosecution where the likelihood of criminality or the validity of the warrant can be tested. The AFP advised me that a DDW is only considered where 'traditional investigative actions are not feasible'.⁴² The Law Council of Australia said that the power enabled police to act as 'judge, jury and executioner'.⁴³ Francis Maxwell has suggested that such a power is 'unprecedented in the democratic world'.⁴⁴

37 *INSLM SLAID Act Report* (n 3) 28 [4.33], citing 'Summary of INSLM Private Hearing with the Australian Federal Police 23 July 2024' (Summary, 23 July 2024) 3 <<https://www.inslm.gov.au/publications/summary-private-hearing-afp-23-july-2024>>; 'Summary of INSLM Private Hearing with the Australian Criminal Intelligence Commission 29 July 24' (Summary, 29 July 2024) 2 <<https://www.inslm.gov.au/publications/summary-private-hearing-acic-29-july-2024>>.

38 Transcript of Proceedings, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth) (SLAID Act)* (Public Hearing, Independent National Security Legislation Monitor, Jake Blight and Jannine Horner, 20 February 2025) 42 (Heather Cook) <<https://www.inslm.gov.au/publications/transcript-public-hearing-20-february-2025>> ('INSLM Public Hearing Transcript').

39 *SD Act* (n 27) ss 6 (definition of 'disrupting data'), 27KE.

40 See *Criminal Code Act 1995* (Cth) sch 1 pt 10.7 ('*Criminal Code*'). Relevant offences include unauthorised modification of data to cause impairment (s 477.2), unauthorised impairment of electronic communication (s 477.3), unauthorised access to, or modification of, restricted data (s 478.1) and unauthorised impairment of data held on a computer disk etc (s 478.2). Relevantly 'unauthorised' is defined in section 476.2 and makes clear that a warrant is capable of authorising police to access, modify or impair data in accordance with the warrant.

41 The Monitor noted that the closest analogy is probably the *Proceeds of Crime Act 2002* (Cth) which allows for civil action to be taken to restrain and recover assets that are suspected to be of criminal origins, even where there has been no criminal conviction or the criminal burden of 'beyond reasonable doubt' has not been met and that unlike that scheme, DDWs do not have judicial oversight or a requirement for court orders before certain actions to deal with property can be taken: *INSLM SLAID Act Report* (n 3) 7 [2.8].

42 AFP Submission (n 18) 5 [25]. Note that the Monitor recommended that the 'last resort' nature of DDWs be encoded in the legislation: Recommendation 13 of the *INSLM SLAID Act Report* (n 3) vii, 164 [11.86]–[11.89].

43 Law Council of Australia, Submission No 21 to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (9 March 2021) 32 [19].

44 Francis Maxwell, 'When Good is Not Good Enough: Evaluating the Proportionality and Necessity of the Australian Government Hacking Warrants' (2022) 34(2) *Current Issues in Criminal Justice* 136, 150 <<https://doi.org/10.1080/10345329.2022.2046934>>.

DDWs cannot be used to cause permanent loss of money, digital currency or property (other than data), but they can certainly have an effect including temporary deprivation.⁴⁵ I was satisfied on the evidence that they have been used to effectively disrupt certain types of cybercrime by the AFP.⁴⁶ The threshold for applying for a DDW is a reasonable belief that disruption of data in a computer will *substantially assist in frustrating* the commission of one or more relevant offences which have been, are being, are about to be, or are likely to be committed.⁴⁷ I recommended that the AFP retain disruption powers but that ACIC (which has never used the power) not.⁴⁸ This recommendation was based on the extraordinary nature of DDWs and the desirability of them being integrated into a law enforcement agency (not an intelligence agency) to ensure that all other lawful ‘disruption’ options, including seizure, arrest and prosecution, were considered and used instead wherever possible.⁴⁹ Separating law enforcement and disruption from intelligence gathering is consistent with the Government’s recent acceptance of a recommendation that ACIC focus on intelligence collection and not have a disruption function.⁵⁰ The Government agreed that ACIC should not retain DDWs.⁵¹

45 *SD Act* (n 27) ss 27KE(7), (12).

46 *INSLM SLAID Act Report* (n 3) 28 [4.33] states that evidence obtained in private hearings included that ‘DDWs have been used for phishing and malware operations. This has helped to protect Australians from these sorts of activities.’

47 *SD Act* (n 27) s 27KA(1).

48 Recommendation 1: *INSLM SLAID Act Report* (n 3) v. The recommendation that the AFP retain DDWs was subject to other recommended improvements to the warrant system being implemented. The ‘Government Response to the *SLAID Report*’ (n 4) 2 said that it ‘agreed’ with Recommendation 1, though in the detail of the response said that it will extend the sunset date for the AFP in respect of DDWs ‘in the first instance, in order to allow recommendations 6–8 to be further considered’ as part of its ongoing electronic surveillance review.

49 The Monitor also recommended the inclusion of a ‘last resort’ test into the issuing criteria for DDWs, specifically that ‘DDWs should only be available when other measures would not be effective’: Recommendation 13 of the *INSLM SLAID Act Report* (n 3) vii.

50 Australian Government, ‘Government Response to the Independent Review of the Australian Criminal Intelligence Commissions and Associated Commonwealth Law Enforcement Arrangements’ (Government Response, November 2024) <<https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/independent-review-ACIC-government-response.pdf>>.

51 ‘Government Response to the *SLAID Report*’ (n 4) 2. The Crimes and Other Legislation Amendment (Omnibus No 1) Bill 2026 (introduced on 11 March 2026) will, if enacted, remove DDWs from ACIC and will extend the current sunset for all *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (*‘SLAID Act’*) warrants for a further three years until 4 September 2029. According to the Explanatory Memorandum, the three-year extension is necessary to allow the Government’s ongoing electronic surveillance review to consider other changes: Explanatory Memorandum, Crimes and Other Legislation Amendment (Omnibus No 1) Bill 2026 (Cth) 12 [41]. In a submission to the Senate Legal and Constitutional Affairs Legislation Committee, I supported removal of ACIC DDWs but noted that it is ‘disappointing’ that electronic surveillance reform is taking so long, and that I am ‘concerned that it is considered necessary to extend the current sunset to late 2029 to await those reforms’: Independent National Security Legislation Monitor, Submission No 2 to Senate Legal and Constitutional Affairs Legislation Committee, Parliament of Australia, *Crimes and Other Legislation Amendment (Omnibus No 1) Bill 2026* (7 April 2026) 2 <https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/CrimeOmnibusNo1Bill2026/Submissions>.

3 Account Takeover Warrants

Account Takeover Warrants ('ATWs') provide authority to take over a person's online account. Taking over an account can include changing a password to prevent a person from regaining access to their account. This is sometimes done to prevent a person from deleting evidence.⁵² However, an ATW is not used to download evidence from an account or to operate the account to obtain evidence, for this another authority such as a controlled operation or a search warrant is used in conjunction with the ATW.⁵³ ATWs can be executed overtly but they can also be exercised covertly so that the subject is unlikely to know that their account has been taken over by authorities.⁵⁴ Because they are not used directly to collect evidence,⁵⁵ and especially if exercised covertly, an ATW is unlikely to be challenged in a proceeding, even if evidence gathered under a related warrant is theoretically challengeable.

4 Related Powers

In addition to the three new warrants, the *SLAID Act* also provided for emergency authorisations. These allow the AFP or ACIC to *internally* authorise the takeover of an account or disruption of data when it is impractical in the circumstances to apply for a warrant and it is necessary to act immediately because of an imminent risk of serious violence or substantial property damage.⁵⁶ These internal authorisations are different to expedited or urgent external authorisation (urgent warrants).⁵⁷

The agencies are also able to obtain assistance orders, which can be used to compel certain people (including non-suspects) to assist in the execution of a warrant.⁵⁸ This can include by providing biometric or other information to unlock

52 *INSLM SLAID Act Report* (n 3) 29 [4.35], summarising AFP reports on the use of ATWs.

53 *Ibid* 38 [5.31] refers to AFP evidence about the use of search warrants to download material from accessed accounts and the potential for controlled operations to be used to operate an account to gather further evidence.

54 *Ibid* 39 [5.34].

55 Revised Explanatory Memorandum, Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (Cth) 15 [29].

56 *Crimes Act* (n 27) s 3ZZUX; *SD Act* (n 27) s 28(1C). I recommended these be retained for the AFP with a minor modification to remove the current prohibition on an external authority reviewing an internally issued emergency authorisation to require destruction of improperly collected information. I also said that as ACIC does not have any emergency response functions, it did not need emergency authorisations: Recommendation 17 of the *INSLM SLAID Act Report* (n 3) ix. The Government 'noted' this recommendation and discussed the need for *law enforcement* agencies to have emergency powers, but did not address the ability to order deletion of improperly collected data, and said that it will 'address the design of emergency and time-sensitive authorisations through the ACIC reform and electronic surveillance reform processes': 'Government Response to the *SLAID Report*' (n 4) 10.

57 Note that the *Crimes Act* (n 27) refers to an 'urgent application' for ATWs: at s 3ZZUN(2); while the *SD Act* (n 27) refers to a 'remote application' for DDWs and NAWs: at ss 27KB, 27KL. They differ in name only. For a discussion on the relationship between 'urgent warrants' (externally issued via an expedited process) and 'emergency authorisations' (internally issued when even an urgent warrant is not practical), see *INSLM SLAID Act Report* (n 3) 192–3.

58 *Crimes Act* (n 27) s 3ZZVG(2)(b); *SD Act* (n 27) ss 64A(6A)(b), 64B(2)(c). See also 'Government Response to the *SLAID Report*' (n 4).

a device or access an account.⁵⁹ I accepted that such powers may be required (though found they had not actually been used) but said that the legislation should be modified so that an order can only be issued when it is proportionate to do so and that issuing authorities be able to add conditions or limits on the order.⁶⁰ The Government ‘noted’ this recommendation and said it would be considered as part of its ongoing electronic surveillance reform project.⁶¹

Having briefly outlined what the powers granted by the *SLAID Act* can authorise, the next question is how well-tailored the powers are and if the safeguards are sufficient. This includes issuing criteria and the system for issuing warrants. Critically, I found that the current system for issuing warrants is not fit for purpose. Before describing my main recommendations for reform of the warrant system, it is useful to first briefly examine the idea of warrants as a *system* and how this framing influenced my approach to analysis in my review of the *SLAID Act*.

III WARRANT ISSUING AS A SYSTEM

Warrants as legal instruments could be described as part of the infrastructure of the law.⁶² They turn an illegal action (such as trespass on property) into a legal action (such as an authorised search). Warrants are powerful legal instruments and play a critical role in authorising surveillance in democracies. There is more than one way to approach a review of legal instruments such as warrants. I was clear from the outset of my review of the *SLAID Act* warrants that I intended this review to be broader than simply looking at the criteria for issuing warrants.⁶³ In the issues paper for the review, I referred to ‘looking at the *system* around the issuing of warrants’.⁶⁴ In the final report I found that the ‘issuing of warrants should not be regarded as a single action that occurs at a moment in time, carried out by an individual. It should be understood as a system that has many interconnected parts’.⁶⁵

The report does not examine what is meant by a ‘system’ or how systems theory informed the review. In this Part of this article, I seek to provide insight into how I incorporated aspects of systems theory into my approach to the review of *SLAID Act* warrants and why this was useful in the praxis of law reform.

59 *INSLM SLAID Act Report* (n 3) 204–5 [14.3].

60 *Crimes Act* (n 27) s 3ZZVG(1); *SD Act* (n 27) ss 64A(1), 64B(1). See also Recommendation 18 of the *INSLM SLAID Act Report* (n 3) ix.

61 ‘Government Response to the *SLAID Report*’ (n 4) 10–11.

62 To borrow the language of Susan Leigh Star, ‘The Ethnography of Infrastructure’ (1999) 43(3) *American Behavioural Scientist* 377, 380–2 <<https://doi.org/10.1177/00027649921955326>>.

63 The 2019 *Comprehensive Review* (n 6) looked at security and some law enforcement warrants amongst other things. The relevant part of that review largely focused on the detail of the criteria for issuing warrants: at ch 28. This is not a criticism of that review, only an illustration of a different and perhaps more traditional approach. The 2019 *Comprehensive Review* (n 6) recommended the current electronic surveillance reform project: see above n 6.

64 ‘Data Disruption, Network Activity and Account Takeover Warrants in the *Crimes Act 1914* and *Surveillance Devices Act 2004*’ (Issues Paper, Independent National Security Legislation Monitor, 7 November 2024) 23 (emphasis in original).

65 *INSLM SLAID Act Report* (n 3) 53.

General systems theory grew from scholars of biology, mechanical engineering and communications (among others) and the desire to have a set of theoretical constructs and tools to promote interdisciplinary work.⁶⁶ Today there is a range of different approaches or schools that fall under the broad umbrella of ‘systems theory’.⁶⁷ These include cybernetics,⁶⁸ systems dynamics,⁶⁹ open systems theory,⁷⁰ and critical systems theory.⁷¹

The use of systems theory in examining law is not new. For example, Richard Nobles and David Schiff have applied the work of Niklas Luhmann, particularly Luhmann’s writings on autopoietic systems, to understand how self-description and self-observation both guide and reinforce the operation of law as a system.⁷² HLA Hart conceived of law as a system of rules which can be distinguished from, and are recognised as distinct from, general social rules, and there is a body of academic scholarship using systems theory, and more recently complexity theory,

-
- 66 Kenneth E Boulding, ‘General Systems Theory: The Skeleton of Science’ (1956) 2(3) *Management Science* 197 <<https://doi.org/10.1287/mnsc.2.3.197>>; Ludwig von Bertalanffy, ‘General System Theory: A New Approach to Unity of Science’ (1951) 23(4) *Human Biology* 302; Norbert Weiner, *Cybernetics: Or Control and Communication in the Animal and the Machine* (Technology Press, 1948).
- 67 See, eg, Magnus Ramage and Karen Shipp, *Systems Thinkers* (Springer London, 2nd ed, 2020) <<https://doi.org/10.1007/978-1-4471-7475-2>>; Ray Ison, ‘Systems Thinking and Practice for Action Research’ in Peter Reason and Hilary Bradbury-Huang (eds), *The SAGE Handbook of Action Research: Participative Inquiry and Practice* (Sage Publications, 2nd ed, 2007) 139 <<https://doi.org/10.4135/9781848607934.n15>>. See, in particular, Figure 9.2 at 144.
- 68 See the early work on cybernetics such as Weiner (n 66); W Ross Ashby, *An Introduction to Cybernetics* (Chapman & Hall, 1956) <<https://doi.org/10.5962/bhl.title.5851>>; Margaret Mead, ‘Cybernetics of Cybernetics’ in Heinz von Foerster et al (eds), *Purposive Systems: Proceedings of the First Annual Symposium of the American Society for Cybernetics* (Spartan Books, 1969) 1. The idea of cybernetics has been translated into a modern Australian context including by Genevive Bell: Genevive Bell, ‘After the Pandemic: Cybernetics Systems and an Approach into the Future’ (Speech, 2021 IPAA National Conference, 29 November 2021); Genevive Bell et al, ‘One Complete System? Telegraphy, Cybernetics and Industrial Archaeology’ (2025) 91(1) *Australian Archaeology* 65 <<https://doi.org/10.1080/03122417.2024.2437190>>.
- 69 See, eg, Jay W Forrester, ‘The Beginning of System Dynamics’ (Speech, System Dynamics Society, 13 July 1989); John Sterman, ‘System Dynamics at Sixty: The Path Forward’ (2018) 34(1–2) *System Dynamics Review* 5 <<https://doi.org/10.1002/sdr.1601>>; Donella H Meadows, *Thinking in Systems: A Primer*, ed Diana Wright (Earthscan, 2009) 153–6.
- 70 See, eg, Ludwig von Bertalanffy, ‘An Outline of General System Theory’ (1950) 1(2) *British Journal for the Philosophy of Science* 134 <<https://doi.org/10.1093/bjps/1.2.134>>; Frederick Edmund Emery and Eric Lansdown Trist, ‘Socio-Technical Systems’ in Charles West Churchman and Michel Verhulst (eds), *Management Sciences: Models and Techniques* (Pergamon Press, 1960) vol 2, 83; David C Benton et al, ‘Use of Open Systems Theory to Describe Regulatory Trends’ (2013) 4(3) *Journal of Nursing Regulation* 49 <[https://doi.org/10.1016/S2155-8256\(15\)30131-9](https://doi.org/10.1016/S2155-8256(15)30131-9)>.
- 71 See, eg, Gerald Midgley, ‘What Is This Thing Called CRITICAL Systems Thinking?’ in Keith Ellis et al (eds), *Critical Issues in Systems Theory and Practice* (Springer, 1995) 61 <https://doi.org/10.1007/978-1-4757-9883-8_7>; Werner Ulrich, *A Primer to Critical System Heuristics for Action Researchers* (Centre for System Studies, 1996); Andreas Fischer-Lescano, ‘Critical Systems Theory’ (2012) 38(1) *Philosophy and Social Criticism* 3 <<https://doi.org/10.1177/0191453711421600>>.
- 72 See, eg, Richard Nobles and David Schiff, *A Sociology of Jurisprudence* (Hart Publishing, 2006) <<https://doi.org/10.5040/9781472563552>>; Richard Nobles and David Schiff, *Observing Law Through Systems Theory* (Hart Publishing, 2013) <<https://doi.org/10.5040/9781472566287>>. See also Jean-Guy Belley, ‘Le Pluralisme Juridique comme Orthodoxie de la Science du Droit’ (2011) 26(2) *Canadian Journal of Law and Society* 257, 269 <<https://doi.org/10.3138/cjls.26.2.257>>.

to describe aspects of the legal landscape and its evolution.⁷³ Systems theory has also been utilised as a tool for contextualising legal problems and evaluating the effectiveness of interventions.⁷⁴ However, the use of systems theory as a *practical* tool for formulating law reform recommendations may be underutilised in institutional law reform in Australia.

Donella Meadows describes a system as an ‘interconnected set of elements that is coherently organised in a way that achieves something’.⁷⁵ By applying what she describes as a ‘systems lens’ to a variety of problems she examines ‘elements’, ‘interconnections’ and ‘function/purpose’ to understand how systems are operating and where there may be opportunities for effective intervention to achieve or strengthen the desired function/purpose. Broadly, this is the definition of a system and the approach I sought to adopt in reviewing the ‘system’ of warrants that underpins the *SLAID Act* powers. At the outset it required analysis of three areas:

- What are the elements of the system?
- How are they connected?
- What is the system currently achieving, and what do I want it to achieve?

These deceptively simple questions were difficult to answer. The process of untangling them provided insights into what had changed about warrants and what needed to change in order to ensure they are an effective safeguard for modern surveillance and related powers.

To identify the ‘elements’ of a system it is necessary to first draw a boundary around the system you are analysing. This sort of ‘boundary analysis’ is an essential element of applying systems theory; it is a tool for differentiating the system of interest from its environment.⁷⁶ At one level the whole apparatus for making, interpreting and enforcing laws is a system.⁷⁷ The ‘business’ of cybercrime could also be cast as a system, as can law enforcement generally or in relation to specific laws. Building on the work of Werner Ulrich,⁷⁸ Gerald Midgley explains that ‘where exactly boundaries are constructed, and what the values are that guide the construction, will determine how issues are seen and what action will be taken’.⁷⁹

73 HLA Hart, *The Concept of Law* (Oxford University Press, 3rd ed, 2012). Cf Charles JG Sampford, *The Disorder of Law: A Critique of Legal Theory* (Blackwell, 1989). On complexity theory and legal issues, see, eg, Jamie Murray, Thomas Webb and Steven Wheatley (eds), *Complexity Theory and Law: Mapping an Emergent Jurisprudence* (Routledge, 2019) <<https://doi.org/10.4324/9781315158976>>.

74 There is some scholarship on using systems theory to understand the context in which law operates and effects of law reform. For example, reform of family court processes based on ‘family systems-theory’ as a way of focusing on effects on families rather than individuals: Susan L Brooks and Dorothy E Roberts, ‘Social Justice and Family Court Reform’ (2002) 40(4) *Family Court Review* 453, 456 <<https://doi.org/10.1111/j.174-1617.2002.tb00854.x>>. For example, systems theory as a conceptual framework for assessing the effectiveness of restorative justice reforms: Sarah Xin Yi Chua and Tony Foley, ‘Implementing Restorative Justice to Address Indigenous Youth Recidivism and Over-Incarceration in the ACT: Navigating Law Reform Dynamics’ (2014–15) 18(1) *Australian Indigenous Law Review* 138, 141–2.

75 Meadows (n 69) 11.

76 Ison (n 67).

77 See, eg, Hart (n 73).

78 Werner Ulrich, ‘A Brief Introduction to Critical Systems Heuristics (CSH)’ (Paper, The Open University, 2006) <https://wulrich.com/downloads/ulrich_2005f.pdf>.

79 Gerald Midgley, *Systemic Intervention: Philosophy, Methodology, and Practice* (Springer, 2000) 36 <<https://doi.org/10.1007/978-1-4615-4201-8>>.

Initially, I framed the system of issuing warrants and how they are connected in what I would describe as a traditional way: an applicant, an application (the provision of relevant information), statutory criteria, an independent decision maker (who weighs the information against the criteria), and a decision. Once I started examining in more detail how they were connected and what the system was achieving or should be achieving, it quickly became apparent that there were many elements missing from my original list. Many of these ultimately became recommendations. These are discussed in more detail in the next section but, briefly, included the lack of a statutory duty of candour connecting the provision of information to the criteria, gaps in information or understanding of complex technology, and gaps in the provision of information on matters of public interest other than law enforcement.

Examining the relationship between elements also provided focus on, for example, what ‘independent’ means in the context of an issuing authority. Issuing warrants is an administrative not a judicial function in Australia, so it does not mean ‘independent of the executive’.⁸⁰ But independence still necessarily includes having the right ‘professional experience and cast of mind’⁸¹ and the ability to act impartially and in an unbiased manner.⁸² This prompted questioning of how a lack of time, training, experience and/or expertise and the absence of any contradictor could easily lead to over-reliance on an applicant’s views.⁸³ It contributed to the recommendation that in future warrants be issued by retired judges who have the experience (including preferably criminal law experience) and time to issue warrants ‘independently’ when supported by technical advice, public interest monitors and an effective secretariat.⁸⁴

In systems theory, feedback loops are essential to balancing and reinforcing systems and importantly they operate on the basis of actual performance rather than expected performance.⁸⁵ Meadows identified feedback loops between different elements of a system, along with access to information, as potential intervention points for affecting change in a system.⁸⁶ An example of how this influenced the findings of the review is the recommendations directed at improving the flow of information between those who independently issue warrants and

80 *Love v A-G (NSW)* (1990) 169 CLR 307, 321 (Mason CJ, Brennan, Dawson, Toohey and Gaudron JJ), affd *Ousley v The Queen* (1997) 192 CLR 69, 80 (Toohey J), 87 (Gaudron J), 100 (McHugh J), 130 (Gummow J); *Grollo v Palmer* (1995) 184 CLR 348 (*‘Grollo’*).

81 *Grollo* (n 80) 367–8 (Brennan CJ, Deane, Dawson and Toohey JJ).

82 Chief Justice Susan Kiefel, ‘Judicial Independence: From What and to What End?’ (Speech, Austin Asche Oration, 27 March 2021) 2–3, cited in Australian Law Reform Commission, *Without Fear or Favour: Judicial Impartiality and the Law on Bias* (Final Report No 138, December 2021) 66. It found that judges, magistrates and ART members are all capable of falling within this description, although the public perception of independence is likely to be higher for magistrates and judges: *INSLM SLAID Act Report* (n 3) 62 [7.19].

83 *INSLM SLAID Act Report* (n 3) 71 [7.55], 73 [7.61], 75 [7.66], 78 [7.76].

84 See Recommendation 6–8: *ibid* v–vi.

85 Vladislav Valentinov, ‘Wiener and Luhmann on Feedback: From Complexity to Sustainability’ (2017) 46(3) *Kybernetes* 386 <<https://doi.org/10.1108/K-11-2016-0317>>.

86 Meadows (n 69).

those who independently assess how warrants are executed.⁸⁷ Currently there is no effective mechanism for those who issue warrants to be aware of systemic problems in the execution of warrants that have been identified by the Inspector-General of Intelligence and Security ('IGIS') or the Commonwealth Ombudsman ('Ombudsman'), nor is there any way warrant-issuers can alert oversight bodies of newly issued warrants that they consider deserve particular scrutiny after execution.⁸⁸ The current lack of any mechanism for such feedback to occur is highlighted as a deficiency in the report.⁸⁹

Access to information is a classic systems intervention point.⁹⁰ Decision-makers can only act on the information put before them, and in ex parte decisions that have adverse implications for rights, it is particularly important that decision-makers are as well-informed as possible. Improving access to information as a mechanism to improve the warrant system underpins central recommendations including the introduction of public interest monitors and a duty of candour.⁹¹ These are discussed further in the next Part of this article.

The elements of the system being examined were further expanded once the 'purpose' of the system was explored.⁹² The *Independent National Security Legislation Monitor Act 2010* (Cth) requires assessment of the effectiveness, necessity and proportionality of a law being examined including its effectiveness in protection of individual rights and ensuring compliance with international obligations (including human rights obligations).⁹³ This informed how I thought about the purpose of warrants. As already discussed, I found that the *SLAID Act* warrants were effective in understanding criminal networks and combating serious crime.⁹⁴ I was not satisfied that the components and operation of the system were effective in ensuring proportionality or protecting rights (particularly privacy rights) as far as possible in the context of achieving the legitimate law enforcement goals. Several recommendations to address this are discussed in the next Part of this article. One example of a recommendation that draws on understanding 'purpose' is my proposal that the effectiveness of policies and procedures for what happens to certain types of information *after* it has been collected should form part of the issuing criteria.⁹⁵ This is not how issuing criteria are currently constructed.⁹⁶ But

87 See Recommendations 7 and 21(a) of the *INSLM SLAID Act Report* (n 3) vi, xi.

88 Ibid 100–03 [8.62]–[8.75].

89 Recommendation 7 of the *INSLM SLAID Act Report* (n 3) proposes a mechanism for such feedback to occur in future: at vi.

90 See Meadows (n 69) 156.

91 See Recommendations 7, 8, 12, 19, 20 and 21 of the *INSLM SLAID Act Report* (n 3) vi–xi.

92 Stafford Beer famously said 'the purpose of a system is what it does' and urged that systems be assessed by reference to their actual outcomes, not stated goals: Stafford Beer, *Diagnosing the System for Organizations* (John Wiley & Sons, 1985) 99.

93 *INSLM Act* (n 1) ss 6, 8. For discussion of international human rights obligations affected by the *SLAID Act* (n 51) warrants, see *INSLM SLAID Act Report* (n 3) ch 17. The right to privacy is the most significantly affected, but other rights examined including the right to a fair hearing, a right to an effective remedy and the prohibition on torture, etc.

94 *INSLM SLAID Act Report* (n 3) 29 [4.36].

95 Recommendations 12(c) and (e): *ibid* vii.

96 *SD Act* (n 27) ss 27KC(1)(a)–(b), 27KM(1)(a)–(aa); *Crimes Act* (n 27) s 3ZZUP(1); *ibid* 141 [11.4]–[11.5].

such a reform supports the purpose of protecting privacy and special categories of information (such as that subject to legal professional privilege) by forcing applicants to explain the likelihood of such information being collected and how they intend to deal with it if it is, bringing these issues to the fore.⁹⁷ The effect will be reinforced by the proposed feedback loop of issuing authorities being informed of any systemic failings in this regard.⁹⁸

A Systems Theory as a Practical Tool for Law Reform

My experience in the *SLAID Act* review was that conceiving of warrant issuing as a system and using articulated values to draw boundaries was of utility for the law reform process because it helped identify and challenge underpinning assumptions. That is, by describing warrants as a system, the system and its components could be iteratively identified and tested against the stated goals of the system in a structured way, in this case whether it acts as an effective safeguard for the exercise of police and criminal intelligence powers. Changes to identified elements of the system and its environment, including changes in technology or capability and the addition or subtraction of new elements in the system can be triggers for review. This broader view of examining a ‘system’ describes what Ray Ison terms a ‘system of interest’ for the purpose of creating a model to achieve change rather than simply describing a system.⁹⁹

Drawing on interdisciplinary research and tools is not new to academic lawyers.¹⁰⁰ There is some research suggesting that while law reform processes remain rooted in traditional doctrinal research methods, there is also some use of interdisciplinary methods.¹⁰¹ I suggest that the approach I took in the *SLAID Act* review is evidence that systems theory offers a range of practical tools that can be used in law reform. I am not contending that utilising systems theory is the *only* way to approach law reform, simply that it can be useful and can provide an analytic structure for some law reform tasks.

97 For example, there was evidence that in New South Wales and Queensland where the Surveillance Devices Commissioner or Public Interest Monitor scrutinises applications and can make submission to issuing authorities, they regularly highlight the risk of material subject to legal professional privilege being collected. Issuing authorities in those jurisdictions routinely make warrants subject to conditions to protect such information, whereas currently, at the Commonwealth level across all warrant types, conditions are very rarely imposed: see *INSLM SLAID Act Report* (n 3) 95 [8.42], 151 [11.40], 157 [11.66].

98 For other specific example of matters identified by oversight bodies which could usefully inform issuing authorities, see *ibid* 100 [8.64], 287–91 annex B.

99 Ison (n 67) 148.

100 See, eg, Douglas W Vick, ‘Interdisciplinarity and the Discipline of Law’ (2004) 31(2) *Journal of Law and Society* 163 <<https://doi.org/10.1111/j.1467-6478.2004.00286.x>>; Bart van Klink and Sanne Taekema, ‘A Dynamic Model of Interdisciplinarity: Limits and Possibilities of Interdisciplinary Research into Law’ (Working Paper No 010/2008, Tilburg University, 9 June 2008); Timothy D Lytton, ‘A Systems Theory of Tort Law: Reevaluating the Case against “Regulation by Litigation”’ (2025) 90(2) *Missouri Law Review* 385.

101 Terry Hutchinson, ‘The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law’ (2015) 8(3) *Erasmus Law Review* 130, 135–8 <<https://doi.org/10.5553/ELR.000055>>.

IV KEY RECOMMENDATIONS FOR REFORM OF THE WARRANT SYSTEM

It should not be a surprise that I found that the current system for issuing warrants is not fit for purpose. The core of the system is over 100 years old and was designed for physical property search warrants, not the kind of covert, intrusive and technology-dependent powers provided for by the *SLAID Act*.¹⁰² What may once have been a significant practical safeguard – the ability to challenge the validity of a warrant in court – has effectively been removed from the *SLAID Act* warrant system because warrants can now be executed remotely and covertly. Individuals whose data has been collected under a NAW, disrupted under a DDW or accessed via a covert ATW, are very unlikely to ever know the information was collected or disrupted using such a warrant, nor with whom the data has been lawfully shared. The chance of material collected under any of these warrants ever being used as evidence in court is very slim, if not remote.¹⁰³ Without a realistic possibility of challenge and thus judicial oversight, much turns on the information given to the decision-maker, their expertise and the criteria for decision-making. I made recommendations for substantial change in each of these areas.

A Independent Technical Advice

As noted earlier, the need for the new powers contained in the *SLAID Act* was described as a response to the growing threat of cyber-enabled and cyber-dependent crime and evidence that traditional ways of gathering evidence and intelligence were becoming ineffective due to encryption and other advanced technologies.

The *SLAID Act* warrants were intended to enable the AFP and ACIC to use new technical capabilities to try and obtain evidence or intelligence about cybercrime. Both ACIC and the AFP gave evidence that specialist skills and capabilities were needed to use the powers. The AFP said that ‘because of the technical expertise and knowledge required’ the use of the warrants was limited to specific commands within the AFP.¹⁰⁴ ACIC explained that they had not used any DDWs or ATWs in the three years the powers had been in effect in part because of the technical complexity and requirement for capability development.¹⁰⁵

102 *INSLM SLAID Act Report* (n 3) 11–13 [2.23]–[2.26]

103 Information collected under NAWs cannot be used as evidence in criminal proceedings, DDWs are intended to be used with traditional mechanisms such as prosecution are not available and ATWs are not themselves used to collect evidence, rather they allow access to an account so that other warrants or powers can be used to extract evidence: *SD Act* (n 27) ss 45B(1), (3), (10); *Crimes Act* (n 27) s 27KC(2)(c); *INSLM SLAID Act Report* (n 3) 38 [5.31].

104 *INSLM SLAID Act Report* (n 3) 24 [4.15], citing INSLM Public Hearing Transcript (n 38) 22 [15] (AFP Deputy Commissioner McCartney).

105 *INSLM SLAID Act Report* (n 3) 24 [4.14]; Australian Criminal Intelligence Commission, Submission No 17 to Independent National Security Legislation Monitor, *Review of the SLAID Act* (10 January 2025) 3 (‘ACIC Submission’).

Technology is evolving rapidly, and organised crime groups are exploiting and adapting new technologies to their advantage, including to avoid surveillance.¹⁰⁶ It must be assumed that law enforcement and intelligence agencies are also rapidly evolving and adapting technology to counter this. The result is that warrants are operating in a technologically complex and dynamic environment and may involve novel or specialised capabilities. The system for issuing warrants has not evolved for this new environment.

The decision-maker issuing warrants needs to be able to independently weigh the risks and the likely impact of a warrant. This goes both to an understanding of what the warrant is actually authorising and the risk of unintended consequences.¹⁰⁷ The technical complexity of operations conducted under *SLAID Act* warrants requires a sophisticated understanding of how warrants are actually executed and risks with the technology involved. This is not something ART members or judges can be presumed to have. I concluded that in today's environment, decision-makers issuing warrants needed to have access to independent technical advice.¹⁰⁸ This adaptation of the current system draws on the experience in the United Kingdom ('UK') where a 'technical advisory panel' has been successfully operating to provide advice to independent warrant authorities for several years.¹⁰⁹ Technical advice is not likely to be required on every warrant, but independent technical advice should be available for warrant-issuers to call on as required and particularly in cases involving new or particularly complex technology

B Public Interest Monitors

In addition to providing access to independent technical advice, another central feature of the proposed new system for issuing warrants is the introduction of public interest monitors ('PIMs').¹¹⁰ A similar role exists at a state level in Victoria,

106 *INSLM SLAID Act Report* (n 3) 17–18 [3.12]–[3.16], citing AFP Submission (n 18) 2 [5], 3 [15]; ACIC Submission (n 105) 2; Attorney-General's Department (Cth), Submission No 20 to Independent National Security Legislation Monitor, *Review of the SLAID Act* (10 January 2025) 3 ('AGD Submission'). Note that the *2024–25 Annual Cyber Threat Report* (n 19) discusses for example the adoption of generative AI as a technology to be used by cybercriminals: at 25.

107 Maxwell (n 44) 146.

108 Recommendation 8(a): *INSLM SLAID Act Report* (n 3) vi. Note that I was not satisfied by evidence from the AFP and ACIC that seemed to suggest that it was unnecessary for the decision-maker to have a strong understanding of the technology that they were authorising for use: at 107–8 [9.5]–[9.10]. The 'Government Response to the *SLAID Report*' (n 4) notes the recommendation about access to independent technical advice and includes it in the matters to be considered as part of the ongoing electronic surveillance reform project: at 5.

109 *Investigatory Powers Act 2016* (UK) ss 246(1)(a)–(b) ('*Investigatory Powers Act*'); *INSLM SLAID Act Report* (n 3) 89–90 [8.14]–[8.21].

110 Recommendation 7 of the *INSLM SLAID Act Report* (n 3) vi. The 'Government Response to the *SLAID Report*' (n 4) indicates that the introduction of PIMs will be considered in the ongoing electronic surveillance review and said that 'Electronic surveillance reform will holistically consider safeguards to ensure alignment for all electronic surveillance warrants and this may include considerations as to the establishment of a Commonwealth PIM. It would be critical to ensure that any Commonwealth PIM does not detract from operational efficiency, or the timely issue of warrants in time-critical operations': at 4. I note there was clear evidence, including from state police services, that PIMs do not cause delay: see *INSLM SLAID Act Report* (n 3) 90–2.

Queensland and New South Wales ('NSW'), and I have placed reliance on the introduction of PIMs at the Commonwealth level to resolve a number of the information deficiencies identified by analysing the current system and to provide a feedback mechanism to enable the system to adapt and evolve over time. While PIMs would not be 'advocates' for the subject of surveillance or disruption in the traditional sense, their role would extend to making submissions on whether the proposed use of power was a necessary and proportionate invasion of rights for all persons who may be affected.

I also envisage that PIMs will provide an effective and efficient 'feedback loop' to both warrant applicants and warrant issuers.¹¹¹ By reviewing draft warrant applications before they go to the issuing authority, the existing state PIM equivalents allow police to rectify any agreed deficiencies or strengthen their case before the warrant application goes to the decision-maker. Over time, this feedback has led to improvements in the quality of applications. It has also led to efficiencies and improvements in police templates and processes.¹¹² The role of state PIMs has been positively commented on in inquiries and cases as well as in submissions from the Inspector of the New South Wales Law Enforcement Conduct Commission and state police to the *SLAID Act* review.¹¹³ I was initially concerned that PIMs may delay warrants and explored the experience of relevant state jurisdiction in this regard. This concern was resolved by clear evidence that PIMs have not added delay.¹¹⁴ There is currently no such role at the Commonwealth level and the only Commonwealth surveillance warrants that state PIMs have a role in are law enforcement-related phone interception warrants in Victoria and Queensland.¹¹⁵

Another missing 'feedback loop' in the current warrant issuing system concerns the information gleaned from post-warrant reports to ministers and the result of oversight inspections (conducted by the Ombudsman and IGIS). Currently, there is no practical mechanism for issuing authorities to know of systemic or other problems identified in such inspections and reports. Nor is there any way for issuing authorities to flag particular warrants for post-execution oversight attention. The *SLAID Act* report cites several publicly reported examples from overseas jurisdictions, as well as some Australian oversight reports, that contain information that appears directly relevant to the proportionality of a warrant

111 The concept and operation of a 'feedback loop' in this sense is borrowed from systems theory: see Valentinov (n 85); Meadows (n 69).

112 *INSLM SLAID Act Report* (n 3) 90 [8.20]–[8.21], 98–9 [8.57]–[8.61].

113 *R v Riscuta* (2017) 266 A Crim R 328, 337 [23] (Burns J); *Heery v Criminal Justice Commissioner* (2000) 110 A Crim R 465, 473–4 [33] (White J); *Royal Commission into the Management of Police Informants* (Final Report, November 2020) vol 4, 185–6. See also extracts from submissions in the *INSLM SLAID Act Report* (n 3) 89–90 [8.16]–[8.21].

114 *INSLM SLAID Act Report* (n 3) 90–2. Commonwealth warrants (unlike most state warrants) also contain separate provisions for the internal issuing of warrants in genuine emergencies, and there is no suggestion that a PIM would be involved before an emergency authorisation is issued. See *INSLM SLAID Act Report* (n 3) ch 13 on emergency authorisations and their difference from urgent warrant applications.

115 Unlike their Victorian and Queensland counterparts, the NSW Surveillance Devices Commissioner has no role in Commonwealth telecommunications interception warrants sought by NSW police, only surveillance device warrants sought under NSW legislation.

application and/or to consideration of the need to apply conditions to a warrant.¹¹⁶ I have proposed that PIMs play a key role in filling this information gap in the system by having access to post-warrant reports and reports by oversight bodies and being able to incorporate relevant findings directly into submissions on relevant warrant applications.¹¹⁷ As occurs under a slightly different arrangement in the UK, there is also potential for PIMs to provide feedback from issuing authorities to oversight bodies on matters of particular concern to issuing authorities or on warrants that are particularly unusual and may benefit from specific oversight attention.¹¹⁸

I expect that, through regular interactions with oversight bodies, police and technical advisors, PIMs will also be well placed to assist issuing authorities to identify matters where independent technical advice may be required.¹¹⁹

In addition to creating feedback loops, PIMs would, as the name suggests, have a role in advocating on public interest matters. While there are public interest issues, such as human rights issues, at stake in all warrants (including traditional physical search warrants), the need for advocacy from a perspective different to that put forward by police or intelligence agencies is particularly important in the case of warrants that can collect a large amount of data covertly, including on people not suspected of committing a crime.

Another area of public interest is the protections applied to particularly sensitive categories of information, including information subject to legal professional privilege or parliamentary privilege, and information about journalists' sources.¹²⁰ Such information may not always be the 'target' of a particular warrant but may well be collected 'incidentally'. As discussed above in Part III of this article, the conscious use of 'boundary analysis' (a tool drawn from systems theory), assisted in recognising that what happens to information *after* it has been collected, including information unexpectedly collected, can be considered part of the

116 *INSLM SLAID Act Report* (n 3) 100 [8.64] includes examples such as agency systems not being set up to delete material that is legally required to be deleted; failure to revoke warrants as required; lack of candour in warrant applications; collection systems recording information that was unexpected/unauthorised; and, whether conditions were complied with.

117 Recommendation 7: *ibid* 100–3 [8.63]–[8.75], vi. As discussed in Part III of this article, information flows between elements of a system are a key part of applying systems theory. See, eg, Meadows (n 69) 156.

118 In the UK, the warrant issuers (judicial commissioners) and inspectors are part of the same agency – the Investigatory Powers Commission ('IPCO'): *Investigatory Powers Act* (n 109). The IPCO also has in-house lawyers who review draft warrant applications and, along with inspectors, provide non-binding guidance. Where judicial commissioners provide comments on warrants, the in-house lawyers ensure that this is communicated to inspectors who then incorporate it in future inspections and reviews: see *INSLM SLAID Act Report* (n 3) 99 [8.58], 100–1 [8.66], citing Email from IPCO to INSLM, 25 July 2025.

119 Recommendation 7: *INSLM SLAID Act Report* (n 3) 98 [8.54]–[8.55], vi. Note that I also recommend that there be no barrier to information sharing among IGIS, the Ombudsman, PIMs and technical advisors (Recommendation 21(a): at xi); and that oversight bodies have access to the proposed technical advisory panel (Recommendation 21 (b): at xi). The 'Government Response to the *SLAID Report*' (n 4) accepted Recommendation 21(a): at 12–13; and said that Recommendations 7 and 21(b) would be considered as part of the Government's ongoing electronic surveillance reform project: at 4, 13.

120 *INSLM SLAID Act Report* (n 3) 94–6 [8.38]–[8.47]. Note that evidence from state PIM equivalents was that legal professional privilege is an issue often raised and one that is frequently the subject of special conditions in warrants issued to state police in those jurisdictions: at 95 [8.42]. In contrast, there was no evidence of such conditions on AFP or ACIC warrants.

warrant issuing *system*. This contributed to the proposal that PIMs have a role in raising issues connected to how ‘unintended’ collection of sensitive information is to be addressed and how long data is retained, what other material it is combined with and how widely it is shared.¹²¹ It also contributed to the recommendation that the proposed new issuing criteria expressly refer to consideration of the treatment of sensitive categories of information after it has been collected.¹²²

There is one existing and very specific mechanism in the *SLAID Act* provisions that is seemingly intended to protect the right to freedom of expression, or at least the public interest in having a free press, though it is of limited effect. Currently, the issuing authority is directed to consider if the public interest in issuing a warrant outweighs the public interest in protecting the confidentiality of journalists’ sources and facilitating the exchange of information with journalists.¹²³ However, this is only enlivened if *each* of the offences for which the warrant is sought is an offence against a secrecy provision.¹²⁴ This means that if any of the matters being investigated involves another crime, including, for example, theft (which is an offence that David McBride was recently convicted of), then the protection does not apply.¹²⁵ Nor would it apply where collection of journalistic source information was incidental to more general police or criminal intelligence investigations. The proposed PIM role would be more flexible and could advocate in relation to freedom of expression and the public interest in having a free press whenever it may be relevant. This, combined with the proposal to extend issuing criteria to consider how sensitive information (including journalists’ information as well as other sensitive categories including medical information) will be dealt with including after it is collected, will provide more robust protections for rights including privacy and freedom of communication.

C Panel of Retired Judges as Issuing Authorities

The question of who should issue warrants was the subject of much deliberation and consultation in this review. This is reflected in the length of the chapter in the report dealing with this one issue.¹²⁶ It is a central issue to the effectiveness of the warrant system, as well as public confidence in the process. It is also one that has much broader ramifications than just *SLAID Act* warrants. I have recommended a major change to current arrangements and the Government has indicated that

121 This potentially goes beyond the remit of the existing state PIM equivalents: see *Police Powers and Responsibilities Act 1997* (Qld); *Public Interest Monitor Act 2011* (Vic).

122 Recommendation 12(c): *INSLM SLAID Act Report* (n 3) vii, 156–61.

123 *Crimes Act* (n 27) s 3ZZUP(2)(dc); *SD Act* (n 27) ss 27KC(2)(ce), 27KM(2)(fa).

124 *INSLM SLAID Act Report* (n 3) 159 [11.70]; *Crimes Act* (n 27) s 3ZZUP(2)(dc)(ii); *SD Act* (n 27) ss 27KC(2)(ce)(ii), 27KM(2)(fa)(ii); Sarah Kendall and Dominic Frost, ‘Network Activity, Account Takeover and Data Disruption Warrants: How Novel Law Enforcement Powers Impact Media Freedom’ (2022) 28(2–3) *Australian Journal of Human Rights* 249 <<https://doi.org/10.1080/1323238X.2022.2135258>>.

125 *INSLM SLAID Act Report* (n 3) 159 [11.71]; *R v McBride [No 4]* [2024] ACTSC 147.

126 *INSLM SLAID Act Report* (n 3) ch 7.

it will consider my recommendation in the context of the electronic surveillance reform project.¹²⁷

One practical consequence of the separation of powers in the *Australian Constitution* is that judges cannot issue warrants in their judicial capacity; if they issue warrants, it must be as '*personae designatae*'.¹²⁸ Since the mid-1990s, judges have been increasingly unwilling to issue warrants and the policy solution to this was to authorise members of the Administrative Appeals Tribunal ('AAT') (now the Administrative Review Tribunal ('ART')) to issue warrants.¹²⁹ In practice, the vast majority of Commonwealth phone interception and surveillance warrants are issued by AAT/ART members and all of the *SLAID Act* warrants examined in the *SLAID Act* review were issued by AAT/ART members.¹³⁰

The ART advised the INSLM in strong terms that warrant-issuing detracts from the time available for members to undertake their core work of making administrative decisions and contributes to the growing backlog of cases.¹³¹ That ART members are selected for administrative, not criminal, law expertise was also noted.

Although the number of *SLAID Act* warrants is modest at present, if all Commonwealth surveillance warrants were required to be issued by judges the workload would be significant – which may in turn reduce the number of judges willing to volunteer to take this role on in addition to their judicial workload.¹³² The number and distribution of magistrates pose practical issues to administering the supporting mechanism that I have recommended be part of a modern warrant issuing system, including access to independent technical advice and submission by PIMs. Furthermore, magistrates are notoriously busy and, like judges, issue warrants as *personae designatae* on top of their ordinary duties, making it difficult to see how they will have sufficient time to consider complex and highly technology-dependent warrant applications thoroughly.

Given the growing workload of the ART and its increasing backlog, it is foreseeable that fewer ART members will be willing to issue warrants, and those

127 'Government Response to the *SLAID* Report' (n 4) 4.

128 *R v Kirby; Ex parte Boilermakers' Society of Australia* (1956) 94 CLR 254, 270 (Dixon CJ, McTiernan, Fullagar and Kitto JJ), 330 (Webb J); *Hilton v Wells* (1985) 157 CLR 57; *Lim v Minister for Immigration, Local Government and Ethnic Affairs* (1992) 176 CLR 1, 26–7 (Brennan, Deane and Dawson JJ); *Grollo* (n 80).

129 AGD Submission (n 106) 9.

130 For example, in 2023–24 there were almost twice as many judges as ART members (61 judges versus 33 ART members) authorised to issue phone interception warrants, but 79% of applicants were made to ART members: *INSLM SLAID Act Report* (n 3) 59 [7.10]. All *SLAID Act* (n 51) warrants (from commencement to 31 December 2024) were issued by ART members. There were 41 ART members and 55 judges authorised to issue *SLAID Act* warrants, though in practice all were issued by a small number of ART members: *INSLM SLAID Act Report* (n 3) 58 tbl 4, 59 [7.9]. ATWs can be issued by any of over 500 magistrates in Australia: at 57 [7.8].

131 *INSLM SLAID Act Report* (n 3) 72–3 [7.59]–[7.60].

132 On average fewer than 20 *SLAID Act* warrants (and renewals) have been sought per year so far. For phone interception warrants the numbers are much greater – over 3,000 per year – and for surveillance device warrants – around 900 per year (including renewals): *ibid* 66 [7.36], 66–7 [7.38], 68 [7.44].

that *are* willing will have less time to do so.¹³³ This is likely to lead to delays for police seeking warrants.

Faced with difficulties in recommending that ART members, sitting judges or magistrates continue to issue warrants, I looked to an alternative model operating in the UK: the use of retired judges to authorise warrants.¹³⁴ Adapted for Australia, I have proposed that a panel of recently retired judges drawn from a range of courts, including state supreme and district courts, be authorised to issue warrants. Retired judges would bring to bear their judicial experience, preferably including criminal law experience, to robustly test warrant applications. Public perception in the scrutiny applied is likely to be served well by the gravitas of using retired judges for such a role. An additional benefit is that, based on the UK experience, police are likely to find that warrant applications are able to be allocated and assessed promptly when there is a dedicated group of issuing authorities available at all times.¹³⁵ It would also make targeted professional development for such a defined group easier.

D Duty of Candour and Independent Allocation of Warrants

I also made recommendations that relate directly to the integrity of warrant applications: that there should be a statutory duty of candour, and that warrant applications should be allocated independently to decision-makers.¹³⁶ To some extent, both of these already exist in some form.

In relation to a duty of candour, I note that it is not the role of the INSLM to audit police applications for candour and no evidence of any lack of candour by Australian authorities was put to me.¹³⁷ However, one purpose of the INSLM review was to look at the overall *system* for issuing warrants and this includes how the law guides interaction between different elements of the system, including the flow of information in the system. It was in this context that the absence of a statutory duty of candour was identified as problematic.

133 Evidence to Senate Legal and Constitutional Affairs Committee, Parliament of Australia, Canberra, 7 October 2025, 122–5 (Michael Hawkins). The Registrar of the ART gave evidence at Senate Estimates that ‘we do not have the staff, member or technological resources to keep up with the demand for our services’: Michael Hawkins, ‘Opening Statement: Administrative Review Tribunal’ (Tabled Document, Senate Legal and Constitutional Affairs Committee, 7 October 2025) 2. The Registrar also advised the Committee that lodgements for administrative review have risen by more than 100 per cent in the last two years and that the backlog has also almost doubled from 66,000 to 112,000 cases and that the Tribunal had around 100 members fewer than it should.

134 *Investigatory Powers Act* (n 109) s 227(2). These provisions allow for sitting or retired senior judges to be appointed as ‘Judicial Commissioners’ whose role includes scrutinising warrant applications: Investigatory Powers Commissioner, *Annual Report of the Investigatory Powers Commissioner 2023* (Report, 20 December 2024) 106. In practice, only retired judges are appointed as judicial commissioners.

135 I was advised by IPCO that, in the UK, when telecommunications data access approvals were centralised in IPCO, the result for police and other agencies that use those powers was that authorisations were able to be obtained faster. The centralised system in the UK has a 24/7 roster of dedicated issuing authorities and a clear process for prioritising urgent requests. Previously these approvals were done internally by police and other agencies: *INSLM SLAID Act Report* (n 3) 194 [13.10].

136 Recommendations 8(b)–(c): *ibid* vi.

137 There was evidence of a lack of candour identified by some oversight bodies in other Five Eyes jurisdictions: *INSLM SLAID Act Report* (n 3) 114 [9.33], 287–91 annex B.

There is a common law duty of candour for warrant applications in the sense that as a matter of administrative law, things that may vitiate the (administrative) decision to issue a warrant, such as fraud, misrepresentation or want of good faith, can be the basis of a challenge.¹³⁸ This is a lower standard than that which applies in *ex parte* court proceedings which relevantly requires ‘actively highlighting things that go against your position’.¹³⁹ The higher standard applies in several states and comparable overseas jurisdictions and is what I have recommended a new statutory duty be based on.¹⁴⁰ Breach of the proposed statutory duty of candour would not require proof of *knowingly* misleading a decision-maker as is required for the offences in sections 137.1 and 137.2 of *Criminal Code*; rather, recklessly providing false or incomplete information would be sufficient to breach the duty. Breach of the duty may go to validity of a warrant and to disciplinary matters but would not, of itself, be an offence.¹⁴¹

As discussed earlier, the likelihood of a *SLAID Act* warrant decision being challenged in court is remote. Thus, the standard of candour would likely never be tested in such a proceeding, arguably meaning it is of little value to amend the legislation to provide a clear and high duty of candour. However, that argument overlooks the overall system of accountability and oversight of warrant applications and the role a statutory duty of candour would play in it. A crucial part of that system is the inspection work of the Ombudsman and IGIS, both of which supported introducing a statutory duty of candour, suggesting it would promote transparency, provide a higher level of assurance and give a ‘legality’ context to inspections.¹⁴² The feedback loop discussed above, that I have proposed between different actors in the system, is designed to enable relevant inspection findings to be incorporated by PIMs in submissions to ensure that those who are deciding warrant applications are aware of any gaps or risks in agency processes for ensuring candour and, should it arise, any concern with candour in a particular application. This process and enhanced inspections should help to avoid the types of failings in duty of candour that have occurred in some comparable jurisdictions, by incentivising agencies to prioritise

138 *Lego Australia Pty Ltd v Paraggio* (1994) 52 FCR 542. Note that review cannot be sought under the *Administrative Decisions (Judicial Review) Act 1977* (Cth) (*‘ADJR Act’*) for any criminal justice process decisions (including a decision in connection with the issue of a warrant) while a prosecution is before the court or any decisions made under the *TIA Act* (n 26): *ADJR Act* (n 138) s 9A, sch 1.

139 *INSLM SLAID Act Report* (n 3) 112 [9.26], citing *Thomas A Edison Ltd v Bullock* (1912) 15 CLR 679, 681–2 (Isaacs J); *Re South Downs Packers Pty Ltd* [1984] 2 Qd R 559, 560 (Campbell CJ); *Lamb v Ariss* [2006] FCA 582, [24] (Sundberg J); *Shinetec (Australia) Pty Ltd v Gosford Pty Ltd* [2024] NSWCA 174, [51] (Ward ACJ, Leeming and Kirk JJA); *Young v Cooke* [2017] NSWCA 33, [27] (Gleeson JA, Macfarlan JA agreeing at [1]); *Aristocrat Technologies Australia Pty Ltd v Allam* (2016) 90 ALJR 370.

140 *INSLM SLAID Act Report* (n 3) 113 [9.30], 114 [9.33], 287–91 annex B.

141 Depending on the facts, corruption or a breach of professional standards may also be relevant: see *National Anti-Corruption Commission Act 2022* (Cth) s 8; *Australian Federal Police Act 1979* (Cth) s 40. Sections 137.1 and 137.2 of the *Criminal Code* (n 40) would continue to apply to knowingly misleading a person charged who is exercising powers or performing functions under a law of the Commonwealth.

142 *INSLM SLAID Act Report* (n 3) 114 [9.35]–[9.36].

their processes to ensure active identification and disclosure of all relevant material, as well as strong record-keeping to demonstrate this has occurred.¹⁴³

Independent allocation of cases to decision-makers is such an ingrained part of the operational independence and integrity of the courts (and the ART) that I found it surprising that there is no requirement that warrant decisions be allocated independently.¹⁴⁴ In practice, the larger ART registries have adopted a roster system for nominated members to review warrant applications, but this is not the case in every ART office or in every court that has judges issuing warrants in a personal capacity. This leaves open the possibility, or at least the perception, that applicants can choose the decision-maker they believe will issue their warrant most easily. This risk is easily overcome with the introduction of a small national-level secretariat with duties that include independent allocation of decisions, case management and rostering and supporting the panel of retired judges.¹⁴⁵

E Issuing Criteria

Warrants are issued in accordance with statutory criteria. I carefully examined the issuing criteria for *SLAID Act* warrants, finding them to be long, complex and at times overlapping, and to also have important gaps. On the assumption that the recommendations about new safeguards, including the use of retired judges, PIMs, access to independent technical advice and a statutory duty of candour, are introduced, I have proposed a significantly streamlined set of issuing criteria. These would consist of an overarching requirement for necessity and proportionality with a non-exhaustive list of six broad considerations to guide decision-makers and help structure warrant applications. The suggested list is:

- nature and gravity of the offences being investigated (or disrupted);
- likelihood that the proposed activity will succeed, as well as the likely value of the resulting intelligence, evidence or disruption;
- extent to which the privacy of *any* person is likely to be interfered with;
- extent to which property rights are likely to be interfered with, including through the introduction of technical vulnerabilities;
- likelihood of special categories of information, *including* information subject to legal professional privilege and information about journalists' sources being collected and, if it is, how the information will be protected; and
- existence of any alternative, less intrusive means of obtaining the information.¹⁴⁶

While most of these seem uncontroversial, it is worth singling out the proposal that the criteria – at the time of issuing – should include how sensitive information

143 In Annex B to the *INSLM SLAID Act Report* (n 3), there are examples from New Zealand, Canada, the UK and the United States where the applicable duties were not satisfied – most were identified through inspections based on a high duty of candour: at 289–91.

144 Rebecca Ananian-Welsh and George Williams, 'Judicial Independence from the Executive' (Conference Paper, Judicial Conference of Australia, July 2014) 11.

145 Recommendations 6 and 8(d) of the *INSLM SLAID Act Report* (n 3) v, vi.

146 Recommendation 12: *ibid* vii. See also at 141–163 [11.4]–[11.82].

(including material subject to legal professional privilege and journalists' sources) will be dealt with *after* it is collected, including if it is collected incidentally. This goes beyond what is arguably the usual consideration at the time warrants are issued, which is what it is the police or intelligence agency *intends* to collect. That traditional approach is underpinned by an assumption that it is only the collection of information that is rights-intrusive, and by a technology-related assumption that the desired data can easily be distinguished from surrounding data at the point of collection. The proposed change recognises both that collection of sensitive data can be incidental, particularly when bulk data needs to be collected, and that what happens after data is collected is potentially at least as rights-invasive, if not more so, than the moment of collection. It also acknowledges that changes in technology mean that it can genuinely be necessary to collect a much larger set of data in order to access and decipher the desired data. Furthermore, it recognises that safeguards that assume data is being collected only for admission as evidence are insufficient – for example, material subject to legal professional privilege might not be admissible in evidence, but that has little application to warrants only used to generate intelligence.

Recognition that data collection has a 'lifecycle', and that regulation may be needed at points in that lifecycle that occur between collection and destruction, is a product of taking a system-level approach to warrants.¹⁴⁷ As I have noted in the report, the impact of advanced analytic techniques such as artificial intelligence ('AI') on privacy and other rights during the lifecycle of data is an area for future review.¹⁴⁸ Changes in technology combined with warrants such as the NAW allow for the covert collection of large amounts of data, including about people not suspected of any wrongdoing, and while there are some restrictions on *disclosure* of that data there are few limits on *use* within an agency and this opens, for example, the possibility of some of this data being used in the training of AI models from which it cannot later be extracted.¹⁴⁹

F Secrecy Provisions

Once information has been collected under a warrant, there are provisions which regulate when it can be disclosed. I have described the secrecy provisions which currently regulate *SLAID Act* warrant information as 'so complex as to be almost impenetrable', noting they run to over 24 pages of legislation, on top of the general secrecy offences in the *Criminal Code* and the specific offences

147 Ibid 166 [12.5], Figure 5. See above Part III for discussion about how the use of systems theory aided in conceptualising, and shifting, the boundaries of the system under consideration.

148 Ibid (n 3) 186 [12.76]–[12.77], noting the recommendation of the *2024 Independent Intelligence Review* that the INSLM review the legislative context around the national intelligence community's use of artificial intelligence to inform legislative and policy changes: Heather Smith and Richard Maude, Department of the Prime Minister and Cabinet, *2024 Independent Intelligence Review* (Report, 21 March 2025) 83.

149 Information obtained under a NAW is to be reviewed at least every five years and destroyed unless it is 'likely to be required in connection with' a broad range of law enforcement and intelligence functions: *SD Act* (n 27) ss 44A, 45B(4), (5), (7), 46AA.

in the enabling legislation for the AFP and ACIC.¹⁵⁰ My critique of the secrecy provisions is consistent with my earlier report and recommendations on general secrecy offences.¹⁵¹ Most of my recommendations from the earlier report on secrecy offences were accepted or accepted in principle by the Government, but the changes are yet to be introduced.¹⁵² The report on the *SLAID Act* warrants presumes that the accepted secrecy recommendations will be legislated.

I have recommended retaining strict limits on when *SLAID Act* information can be used, but doing so as a positive list of limited permissions, rather than as a convoluted set of exceptions to a series of specific offences. In my view, reliance should be placed on the general secrecy offences in the *Criminal Code* to deal with most unauthorised disclosure. I also made specific recommendations intended to ensure that the law does not improperly restrict the disclosure of potentially exculpatory material or limit access to legal advice, and to clarify that NAW related material cannot be used in proceeds of crime applications.¹⁵³ One of these, the recommendation to ensure that exculpatory material obtained under a NAW can be disclosed in accordance with the usual prosecutorial duty of disclosure, has already been enacted.¹⁵⁴

G Other Key Recommendations

In addition to the three central recommendations about improvements to the warrant issuing system,¹⁵⁵ and the associated recommendations about simplified issuing criteria and secrecy,¹⁵⁶ I have recommended raising the threshold for offences that warrants can be sought for to only those that attract a minimum penalty of at least five years imprisonment.¹⁵⁷ This supports the objective of the rights-invasive powers being focused only on prevention and disruption of *serious* crime.

¹⁵⁰ *INSLM SLAID Act Report* (n 3) 125 [12.11].

¹⁵¹ Jake Blight, Independent National Security Legislation Monitor, *Secrecy Offences: Review of Part 5.6 of the Criminal Code 1995* (Report, 27 June 2024).

¹⁵² Australian Government, 'Australian Government Response to the Independent National Security Legislation Monitor Report: Secrecy Offences' (Government Response, 27 November 2024). See also *INSLM Annual Report 2024–25* (Report, 3 November 2025) 21.

¹⁵³ Recommendation 12 of the *INSLM SLAID Act Report* (n 3) vii.

¹⁵⁴ *TOLA Act* (n 21) sch 1.

¹⁵⁵ Recommendations 6, 7 and 8 of the *INSLM SLAID Act Report* (n 3) v–vi.

¹⁵⁶ Recommendations 12 and 14; *ibid* vii–viii. See also Recommendation 13 that there be additional issuing criteria to ensure data disruption warrants are only issued as a last resort: at vii. The 'Government Response to the *SLAID Report*' (n 4) indicates that Recommendations 12 and 13 along with 14(a), (b), (c) and (f) will be considered as part of the ongoing electronic surveillance review: at 6–8. Recommendations 14(d) and (e) were 'agreed': at 8. Recommendation 14(d) relates to removing barriers to a person seeking legal advice on an assistance order. Recommendation 14(e) recommended permitting potentially exculpatory material obtained under a NAW to be discussed in accordance with the usual prosecutorial duty of disclosure. This recommendation was given effect by urgent amendments made in the *TOLA Act* (n 21) which commenced on 5 November 2025.

¹⁵⁷ Recommendation 9 of the *INSLM SLAID Act Report* (n 3) vi. The current threshold is three years plus some lesser offences: at 126–132 [10.3]–[10.26]. The 'Government Response to the *SLAID Report*' (n 4) indicates that this recommendation will be considered as part of the ongoing electronic surveillance review and that the same threshold was recommended by the *2019 Comprehensive Review* (n 6): 'Government Response to the *SLAID Report*' (n 4) 5–6. The response also suggested that a different threshold was being considered for ACIC.

With these additional safeguards, or at least the three central recommendations which would see the switch to use of retired judges as issuing authorities (or if that is not accepted, then only sitting judges), the introduction of PIMs and independent technical advice, I recommended not only retaining the *SLAID Act* warrants,¹⁵⁸ but also expanding them in two ways. The first would be to allow account takeover warrants to be issued in relation to a ‘named person’ rather than a list of specific accounts.¹⁵⁹ This was sought by the AFP to address situations where additional accounts are identified once a search has begun and there is a real risk that a suspect (or someone on their behalf) could delete the accounts or data could be triggered to self-delete before a further warrant, even an urgent warrant, could be sought.¹⁶⁰ The second expansion would be to allow NAWs to be sought for up to six months at a time, rather than the current 90 days, in light of evidence that intelligence gathering activities of this type are often complex and long-running operations.¹⁶¹

The recommended extension of NAWs to up to six months was subject to the new warrant system proposed in Recommendations 6–8 being implemented and also a requirement that a mechanism be introduced to ensure reporting on warrants occurs at least every six months.¹⁶² The latter highlighted a gap in the current ministerial reporting scheme that only requires reporting when a warrant has concluded – which may be after many years in the case of warrants renewed multiple times. Other gaps in both ministerial and public reporting were also described in the report and recommendations made to enhance both,¹⁶³ notwithstanding a submission by the Attorney-General’s Department questioning the utility of reporting to ministers.¹⁶⁴

There was also a set of recommendations directed at providing clearer boundaries for associated powers, including urgent and emergency warrants and assistance orders.¹⁶⁵ This includes a recommendation that emergency (internal) authorisation be retained for the AFP, given the role of police as ‘first responders’,

158 Recommendation 1–3 of the *INSLM SLAID Act Report* (n 3) v. Note that the ‘Government Response to the *SLAID Report*’ (n 4) ‘accepted’ Recommendations 1–3, but the detail of the response indicated that this means the sunset date for the warrants will be extended while the Government gives further consideration to the proposed changes to the warrant system including the key Recommendations 6–8: at 2–3.

159 Recommendation 4 of the *INSLM SLAID Act Report* (n 3) v. The ‘Government Response to the *SLAID Report*’ (n 4) indicates that this recommendation will be considered as part of the ongoing electronic surveillance review and that it is seeking to ‘ensure consistency across the entire electronic surveillance framework’: at 3.

160 *INSLM SLAID Act Report* (n 3) 41–42 [6.5]–[6.9].

161 Recommendation 5: *ibid* v, 46 [6.24]–[6.26], 50 [6.37]–[6.41].

162 Recommendation 5: *ibid* v. The ‘Government Response to the *SLAID Report*’ (n 4) ‘agreed’ to this recommendation. However, the text of the response suggests the ‘agreement’ is to the extension and not necessarily the caveat about the additional safeguards and reporting being required: at 3–4.

163 Recommendations 19 and 20 of the *INSLM SLAID Act Report* (n 3) ix–x. The ‘Government Response to the *SLAID Report*’ (n 4) 11–12 noted both of these recommendations, saying they would be considered as part of the ongoing electronic surveillance project and in relation to ministerial reporting by ACIC as part of the ACIC reform proposal.

164 *INSLM SLAID Act Report* (n 3) 216 [15.11]; AGD Submission (n 106) 26.

165 Recommendations 11, 17 and 18 of the *INSLM SLAID Act Report* (n 3) vi, ix. The ‘Government Response to the *SLAID Report*’ (n 4) 6, 9–10 noted these recommendations and says they will be considered part of the ongoing electronic surveillance project.

but that it was not necessary for ACIC to have such powers for intelligence gathering operations.

Recommendations to improve the efficiency of oversight include allowing oversight bodies to make use of the proposed technical advisory panel and removing prescriptive requirements to give the Ombudsman more flexibility in determining inspection priorities.¹⁶⁶ Another oversight recommendation was to remove prescriptive statutory record-keeping and notification requirements, and replace them with a scheme allowing administrative guidance to be given on when agencies have to notify about the use of certain powers and what records they are required to keep.¹⁶⁷ This increase in flexibility has similarities to recommendations which propose binding administrative guidance be used to increase the certainty and transparency of requirements relating to the review and deletion of data holdings, and provision of enhanced protections for sensitive categories of information.¹⁶⁸ The use of administrative guidance of this type in the UK has included publication of detailed codes of practice.¹⁶⁹

V BROADER IMPLICATIONS OF THE INSLM REPORT

A Broader Implications of the INSLM Review

In addition to the direct implications of my report on the future of *SLAID Act* powers, the report has at least two possible broader implications. The first is as a potential trigger for the wider use of systems theory as a practical tool in law reform processes. As discussed in Part III of this article, the process of this review demonstrates that there is potential for the application of systems theory to aid practitioners of law reform. There is a need for further research on the practical application of systems theory tools to the process of law reform.

The second and perhaps more obvious implication is that although my *SLAID Act* report recommendations strictly only apply to the *SLAID Act* powers,¹⁷⁰ they

166 Recommendation 21(c) of the *INSLM SLAID Act Report* (n 3) xi. The ‘Government Response to the *SLAID Report*’ (n 4) noted this recommendation and ‘acknowledges that a closer alignment between the Ombudsman’s inspection powers under the *SD Act* and its investigation powers under the *Ombudsman Act 1976* would be beneficial in ensuring the Ombudsman has flexibility in its oversight of the use of *SLAID Act* powers’: at 13.

167 Recommendation 21(d): *INSLM SLAID Act Report* (n 3) xi. The ‘Government Response to the *SLAID Report*’ (n 4) 13 noted this recommendation and that the *2019 Comprehensive Review* (n 6) ‘also considered that legislation and/or guidelines should be clear about record-keeping requirements, to support meaningful oversight’.

168 Recommendations 15 and 16 of the *INSLM SLAID Act Report* (n 3) viii. The ‘Government Response to the *SLAID Report*’ (n 4) 9 noted these recommendations and said they would be considered as part of the electronic surveillance reform project and ACIC reforms.

169 In the UK, Codes of Practice are issued by the Secretary of State under the *Investigatory Powers Act* (n 109).

170 This is because the boundaries of the review were determined by the specific requirement that this review be conducted in s 6(1B) of the *INSLM Act* (n 1). After this review was completed, the *Strengthening Oversight of the National Intelligence Community Act 2025* (Cth) has amended the scope of the INSLM’s own motion powers. See the new definition of ‘counter-terrorism and national security legislation’ in s 4A of the *INSLM Act* (n 1).

have clear implications for other electronic surveillance warrants and the long-running government electronic surveillance reform project. This was recognised in the Government response to the report which said that:

The Monitor also made a number of recommendations relating to enhancing the system for issuing warrants and improving the safeguards that apply to SLAID Act powers, but are also common to all electronic surveillance warrants.

In response to the Monitor's 21 recommendations, the Government has agreed to 4 of those recommendations, agreed to 2 recommendations in part, and noted the remaining 15. The Government will further consider the recommendations that have been agreed in part or noted, as part of electronic surveillance reform, as these recommendations are applicable to the electronic surveillance framework as a whole. The four recommendations accepted by the Government included contingent recommendations from the INSLM—they contemplate other recommendations (namely recommendations 6–8) also being implemented. Those other recommendations have been noted and will be considered during electronic surveillance reform, given their potential applicability to a wide range of electronic surveillance powers.¹⁷¹

The key message from my report is that modern, powerful and invasive warrants require modern, powerful and meaningful safeguards, and in particular, there is a need to modernise the warrant issuing system. Without such safeguards, there is a real risk of loss of the public trust essential to license such significant privacy invasions by law enforcement and criminal intelligence agencies. There is also a real risk that Australia may not meet its *ICCPR* privacy and other human rights obligations.¹⁷² I am pleased that the Government has responded to my report and that the recommendations have been recognised as having application to all electronic surveillance powers.

The assumption that, as was the case decades ago, administratively issued search warrants would ultimately be subject to judicial scrutiny, either as part of the evidence process or in the form of an injunction or other order, no longer holds true. Covert warrants, intelligence warrants and any warrant that allows the collection of bulk data are unlikely to be scrutinised in this way. Due to changes in technology, warrants have the potential to collect vast amounts of data. Even phone interception warrants have changed as technology has changed – a warrant that once allowed listening to phone calls one at a time, making a cassette recording and typing out a transcript using carbon paper to make a copy, now allows the interception of a broadband connection and collection, analysis and dissemination of digital data at a scale and speed unimaginable when the warrants were first introduced.¹⁷³ The key safeguards, including the system for issuing warrants, have not kept pace.

This problem is particularly acute for *SLAID Act* warrants which can authorise the covert collection of vast amounts of data and allow other significant intrusions

171 'Government Response to the *SLAID* Report' (n 4) 1.

172 Brendan Walker-Munro, Ruby Ioannou and David Mount, 'Privacy and Hacking Powers: Is There an Implied Right to Privacy in the Use of Computer Surveillance Powers in Australia?' (2024) 12(1) *Salus Journal* 31.

173 Jake Blight, 'ASIO Telecommunications Interception and Data Access Powers' (2023) 48(4) *Alternative Law Journal* 288.

on rights through the takeover of online accounts and the deliberate alteration or disruption of data. But these are not the only warrants where significant rights invasions are permitted on the basis of outdated assumptions.

B A Practical Approach

Taking account of the constitutional restraint on judges who exercise federal judicial power issuing warrants other than in their personal capacity, as well as the practical implications of diversion from core functions for both judges and ART members and the increasing risk of delay for police seeking warrants, the proposal to utilise a panel of retired judges is a practical one. Recently retired judges, particularly those with years of experience in criminal law, have the skills – and likely the time and willingness – to bring robust scrutiny to applications. The UK experience of having dedicated issuing authorities has ultimately been welcomed by police, as it has both increased the speed at which applications are processed and enhanced public trust in the scrutiny process.¹⁷⁴ The approach is likely to be cost-effective – especially when considered in the scale of the cost of serious and organised crime, and the investment in police and intelligence surveillance capabilities.¹⁷⁵ Similarly, the use of PIMs and a technical advisory panel is likely to bring significant value in terms of both efficiency and effectiveness at a low cost.

Increasing flexibility through streamlined warrant issuing criteria and a move to binding administrative guidance for some details such as notification requirements and data review processes is pragmatic and likely to be welcomed by agencies, though care will need to be taken that this does not reduce transparency and is not implemented in isolation from the broader reforms needed.

VI CONCLUSION

My review of the *SLAID Act* recognises that cyber-enabled and cyber-dependent crime are a significant challenge, and that law enforcement and criminal intelligence agencies need new surveillance, account-takeover and disruption powers to combat it. The recommendation to retain, and in some modest ways to expand, those powers has one significant caveat: the current safeguards are inadequate, even for retaining the powers as they are.

¹⁷⁴ *INSLM SLAID Act Report* (n 3) 194 [13.10] n 717.

¹⁷⁵ The cost of serious and organised crime in Australia in 2022–23 was estimated to be between \$30.4 billion and \$68.7 billion: Russell G Smith, *Estimating the Costs of Serious and Organised Crime in Australia, 2022–23* (Statistical Report No 50, 19 December 2024). The cost of the development and use of electronic surveillance capabilities by police and intelligence agencies is not separately itemised in their budgets. Expenditure specifically on telecommunications interception for 2023–24 is listed in the *2023–24 Annual Report under the Telecommunications (Interception and Access) Act 1979 and Part 15 of the Telecommunications Act 1997* (Report, 2023–24) 37–9 tbls 22, 23. This reports almost \$4.8 million for ACIC and \$22.6 million for the AFP. These figures do not include *Crimes Act* (n 27) warrants or *SD Act* (n 27) warrants and would not include the cost of developing or maintaining capability associated with *SLAID Act* (n 51) or other warrants issued under those Acts. Nor do they include the cost of acquisition and licensing of software systems to process and manage intelligence and analytic capabilities.

I have called for a significant overhaul of the century-old system for issuing warrants and demonstrated that many of the assumptions the old system is based on no longer hold true. As elements of the system have changed over time because of things such as changes in technology, changes in issuing authorities and the reduced role of judicial review, we have not consciously viewed and reviewed the warrant process as a *system* made up of interconnected elements that needs adjustment so that it can continue to meet its purpose as an effective safeguard against overbroad use of powers. To ensure compliance with the *ICCPR* and to maintain public trust in there being a robust system for ensuring privacy and other rights are only invaded where necessary and proportionate, changes are needed. The proposed new system, underpinned by the introduction of PIMs, availability of independent technical advice and a dedicated group of warrant issuers made up of retired judges is practical and achievable. Other recommended changes, including to issuing criteria, secrecy and oversight, are important, but unless changes to the system for issuing warrants are implemented, they will not be sufficient safeguards.