Human Rights Law Centre

Submission regarding the review into the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*

17 December 2024

Human
Rights
Law
Centre

Kieran Pender
Associate Legal Director

Human Rights Law Centre
Level 17, 461 Bourke Street
Melbourne VIC 3000

T: + 61 3 8636 4450
F: + 61 3 8636 4455
E: admin@hrlc.org.au
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses strategic legal action, policy solutions and advocacy to support people and communities to eliminate inequality and injustice and build a fairer, more compassionate Australia. We work in coalition with key partners, including community organisations, law firms and barristers, academics and experts, and international and domestic human rights organisations.

We acknowledge the lands on which we work and live, including the lands of the Wurundjeri, Bunurong, Gadigal, Ngunnawal, Darug and Wadawurrung people. We pay our respect to Elders of those lands, both past and present.

We recognise that Aboriginal and Torres Strait Islander people and communities were the first technologists and innovators on this continent, with deep knowledge systems that continue to shape our understanding of innovation, sustainability, land stewardship, and community care. We recognise that this land always was and always will be Aboriginal and Torres Strait Islander land because sovereignty has never been ceded.

We acknowledge the role of the colonial legal system in establishing, entrenching, and continuing the oppression and injustice experienced by First Nations peoples and that we have a responsibility to work in solidarity with Aboriginal and Torres Strait Islander people to undo this.

We support the self-determination of Aboriginal and Torres Strait Islander peoples.

Follow us at http://twitter.com/humanrightsHRLC

Join us at www.facebook.com/HumanRightsLawCentreHRLC/

Contents

1. Executive Summary

The Human Rights Law Centre (**Centre**) thanks the Independent National Security Monitor (**INSLM**) for the opportunity to make a submission regarding the review into the amendments made by the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021* (Cth) (***SLAID Act***).

The primary purpose of the *SLAID Act* was to amend the *Surveillance Devices Act 2004* (Cth) (***Surveillance Devices Act***) and *Crimes Act 1914* (Cth) (***Crimes Act***) to give officers of the Australian Federal Police (**AFP**) and Australian Criminal Intelligence Commission (**ACIC**) access to three new types of surveillance warrant:

- a **Data Disruption Warrant**, which enables the AFP and the ACIC to access data on one or more computers and perform disruption activities;
- a **Network Activity Warrant**, which enables the AFP and the ACIC to collect intelligence on online activities; and
  an **Account Takeover Warrant**, which enables the AFP and the ACIC to take over a person's online account (collectively, **the Warrants**).

The Centre opposed the implementation and use of the Warrants when the *SLAID Act* was first tabled for discussion, making a submission into the bill's inquiry as well as appearing before the parliamentary committee.[1] Upon the *SLAID Act* coming into law, we further noted our disappointment that these new surveillance powers had the potential to stifle fundamental aspects of a free and open democratic society.[2]

At each of those junctures, we expressed our concerns regarding the disproportionate nature of the powers afforded to the AFP and the ACIC, and how those powers would encroach on the fundamental human rights of all Australians, particularly in the absence of an overarching human rights framework in Australia.

This INSLM review provides an opportunity for the Centre to restate its stance with the hindsight of three years' operation of these additional surveillance powers, and to again propose redressing measures with a view to better balancing these new powers with the fundamental rights and freedoms of all Australians.

[1] Human Rights Law Centre, Submission No 15 to the Parliamentary Joint Committee on Intelligence and Security, *Review of the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020* (18 February 2021); Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 10 March 2021.
[2] Human Rights Law Centre, 'Insufficient safeguards in new surveillance law', *News* (Web Page, 25 August 2021) <https://www.hrlc.org.au/news/2021/8/25/insufficient-safeguards-in-new-surveillance-law>.

2. Summary of recommendations

The Centre **recommends** that the INSLM, following its inquiry, recommend the following changes in relation to the operation of the Warrants:

1. A public interest monitor should be available to review applications and assist independent issuing authorities.
2. Such a public interest monitor should be provided with information about how the Warrants are used in practice and the outcomes of thematic reviews or inspections by oversight bodies in order to better inform the execution of the monitor's role.
3. The Warrants should only be available when other avenues to achieve the same results have been exhausted.
4. Both a new category qualifier and a heighted severity qualifier should be imported into the definition of "relevant offence".
5. The terms "criminal network of individuals" and "electronically linked group of individuals" should be narrowed to require that each individual in the group be engaged in or facilitating conduct that constitutes a relevant offence (whether knowingly or not).
6. Clear processes regarding the handling of information collected under the Warrants should be implemented. These should include a requirement to review and destroy any information that is no longer relevant after a period of three years.
7. Mandatory public report requirements in relation to arrests and prosecutions pursuant to the Warrants should be enacted and made unambiguous.
8. Recommendation 80 from the 2019 Comprehensive Review, namely that electronic surveillance should only be authorised where it is necessary for, and proportionate to, the purposes of an investigation, should be fully implemented.

3. Surveillance and human rights

As expressed in our original submission to the Parliamentary Joint Committee on Intelligence and Security, the Centre remains concerned about the disproportionate scope of the Warrants and the lack of evidence justifying the need for powers of this nature beyond those already available to the AFP and ACIC prior to the implementation of the *SLAID Act* – especially given the absence of an overarching, robust human rights framework.

The Warrants enable the AFP and the ACIC to undertake significant invasions of privacy in the investigation of suspected criminal activity. This is particularly so in the case of the Network Activity Warrant, which provides law enforcement the ability to access and monitor a range of devices with a potential connection to criminal activity, as well as the Account Takeover Warrant, which grants law enforcement the power to alter and remove individuals' access to their online accounts.

These powers threaten to encroach on every Australian's fundamental human right to privacy.[3] It is well established that any limitation on non-absolute human rights must be necessary and proportionate,[4] and it is our view that, absent safeguards provided by both a sufficiently powerful oversight mechanism and an overarching Human Rights Act, the circumstances under which the Warrants may be issued and the powers they provide give rise to opportunities for disproportionate invasions of privacy.

Indeed, as acknowledged in the 2019 Comprehensive Review:

> *Article 17 of the International Covenant on Civil and Political Rights provides that interferences with privacy must be necessary to achieve legitimate purposes and proportionate to those purposes. Settled international case law provides that the principle of proportionality requires that acts are appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives.*[5]

Importantly, the 2019 Comprehensive Review recommended that law enforcement agencies did not require new intrusive powers, such as those provided via the Warrants, to combat cyber-related crime.[6] As part of its rationale, the 2019 Comprehensive Review identified a number of principled problems with such an approach, including the fact that conferring a data disruption power on the AFP "risks compromising essential democratic rights"[7]:

> *Police making conclusive assessments of criminality would raise serious questions about the separation of powers, given that the courts, not police, are responsible for adjudicating criminal guilt in Australia. Such a move should not be taken lightly—it is the equivalent of making the police the judge, jury and executioner, and this would have fundamental consequences for the rule of law in Australia.*[8]

One of the most effective ways to temper otherwise unbridled state surveillance is via strong human rights guardrails. Indeed, the application of human rights frameworks and oversight mechanisms does much to secure the legitimacy of otherwise covert powers.[9]

As noted in the INSLM Issues Paper, the range of offences for which the Warrants can be engaged at present is much too broad.[10] This only diminishes confidence in the Warrants being necessary and proportionate surveillance tools.

---

[3] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17.
[4] See, eg, Australian Human Rights Commission, 'Lawful Limits on Fundamental Freedoms, *Human Rights Brief No. 4* (Web Page, 8 March 2006) <https://humanrights.gov.au/our-work/publications/human-rights-brief-no-4>.
[5] Dennis Richardson, *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Final Report, December 2019) vol 2, 47 [18.59] (**2019 Comprehensive Review**).
[6] Ibid vol 3, 218-21 [38.58]-[38.76].
[7] Ibid 220 [38.70].
[8] Ibid 221 [38.73].
[9] See David Anderson, 'National Security and Human Rights' (Speech, Denning Society Lecture, Lincoln's Inn, 27 November 2024) 11 [34].
[10] Independent National Security Legislation Monitor, 'Issues Paper: Data disruption, network activity and

We also have heightened concerns regarding the use of Warrants in contexts that could degrade the integrity of our democracy, for instance in relation to whistleblowers, journalists and lawyers. The breadth of the scope of the Account Takeover Warrant means that the Warrants can be used to target the activities of individuals acting in the public interest, such as whistleblowers. For example, under the current regime a warrant can be deployed where:

- a person posts content on social media that is deemed menacing, harassing or offensive;[11]
- a whistleblower communicates information obtained under a surveillance warrant in a way that prejudices an investigation;[12]
- a whistleblower discloses information relating to the "assistance and access" regime in the *Telecommunications Act*;[13] and
- a lawyer or journalist assists a government whistleblower to uncover wrongdoing, in a manner deemed to constitute "incitement".[14]

The above concerns underpin the basis for our responses over the ensuing sections of this submission, which address specific questions posed in the INSLM Issues Paper.

account takeover warrants in the *Crimes Act 1914* and *Surveillance Devices Act 2004* (Issues Paper, 7 November 2024) 37-8 [5.8]-[5.14] (**INSLM Issues Paper**).

[11] *Criminal Code Act 1995* (Cth) s 474.17.

[12] *Surveillance Devices Act* s 45(2).

[13] *Telecommunications Act 1997* (Cth) s 317ZF.

[14] *Criminal Code Act 1995* (Cth) s 11.4.

4. Questions raised in INSLM Issues Paper

4.1 Public interest monitor and SLAID power information

[4.47.3] Should there be some sort of public interest monitor (PIM) available to review applications and assist independent issuing authorities?

[4.47.4] Would it support the work of issuing authorities (or PIMs) to be provided with information about how SLAID powers are used in practice and the outcomes of thematic reviews or inspections by oversight bodies?

The Centre welcomes safeguard and oversight mechanisms which protect against exercises of power that arbitrarily intrude on human rights.

The INSLM Issues Paper notes that there were several submissions which called for a public interest monitor or contradictor in relation to the Warrants.[15] In particular, the Parliamentary Joint Committee on Human Rights stated that a PIM or similar mechanism would be a "valuable safeguard to protect the interests of the affected person in any warrant application or review proceedings,"[16] which is a position the Centre shares.

We also note that, while not necessarily causative, proportionally less warrants were sought and issued in Victoria and Queensland (where there is a public interest monitor) compared to NSW (where the Surveillance Devices Commissioner currently has no role in interception warrants).[17] Further, from a qualitative perspective, the comments made by the Registrar of the AAT indicate that those members who were tasked with issuing warrants generally feel that PIMs provide for a more precise system.[18] Consequently, there are viable indications that PIMs both objectively and subjectively improve the quality and exactness of the issuing system, and better align the Warrant regime with the principle of proportionality.

In this vein, providing such a PIM with information regarding how the Warrants are used in practice will assist the PIM in making informed decisions regarding whether or not Warrants have been and continue to be used in the public interest. Importantly, this will provide the PIM with opportunities to calibrate and inform its ongoing approval and review powers regarding these relatively new, invasive powers.

This recommendation is consistent with our prior position, in this and other contexts, in favour of monitors and special advocates in circumstances where a party is not in a position to advocate against the curtailment of their rights and freedoms.

Recommendation 1: A public interest monitor should be available to review applications and assist independent issuing authorities.

Recommendation 2: Such a public interest monitor should be provided with information about how the Warrants are used in practice and the outcomes of thematic reviews or inspections by oversight bodies in order to better inform the execution of the monitor's role.

4.2 Safeguards

[5.35.1] Do the current issuing criteria provide sufficient safeguards or are changes required?

The current issuing criteria do not provide sufficient safeguards.

---

[15] INSLM Issues Paper (n 10) 29 [4.25].
[16] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human rights scrutiny report* (Report No 3, 17 March 2021) 94 [2.91], 98 [2.103(f)].
[17] INSLM Issues Paper (n 10) 32 [4.35].
[18] Ibid 33 [4.40].

The Warrants should only be used if there are no less intrusive means available of achieving the desired result. Although this comprises one of the issues to be considered in relation to granting Network Activity Warrants,[19] it is but one of several competing considerations. The Centre's view is that, given how extraordinary these powers are, the only proportionate way in which the Warrants can be used, including Network Activity Warrants, is for them to be available *only* in circumstances where there is no other alternative less intrusive means of achieving the desired result. Only once these other avenues have been exhausted should the Warrants be something that the AFP or the ACIC can seek to employ.

In relation to the threshold question of "relevant offences" – the Centre welcomes the fact that the INSLM noted this as "one of the most significant issues in the inquiry."[20] This issue was discussed at length in the INSLM paper, [21] and the Centre was cited on this point.[22] Put simply, the types of offences for which the Warrants can be issued is far too broad.

The Centre's position is that *both* a category qualifier (requiring that relevant offences relate to specific serious subject matter) and heightened severity qualifier (ideally raising the bar of relevant offences to those punishable by a period of imprisonment greater than the at-present three years) should be implemented, meaning that a narrower, more targeted tranche of offences would enliven the ability to issue one of the Warrants. This approach better aligns with the principle of proportionality, as powerful tools such as these Warrants should only ever be used to address specific, serious issues. This in turn bolsters the legitimacy of these laws – ultimately, the expansion of state surveillance has a democratic cost, which can only be mitigated by ensuring that the use of any expanded power is necessary and proportionate.

In relation to journalists, while there are additional issuing criteria to be considered if a warrant involves a journalist (or their employee) as provided in the INSLM Issues Paper,[23] this ultimately falls short of the recommendation made by the Parliamentary Joint Committee of Intelligence and Security that a "public interest advocate" be appointed in relation to any applications regarding journalists or media organisations.[24] This discrepancy can ultimately be remedied, and better protections afforded to journalists and media organisations, by implementing an overarching PIM as recommended in section 4.1 above.

Network Activity Warrants are also particularly broad, and pose an outsize risk to the work of both journalists and whistleblowers. We have previously stated that the definitions of "criminal network of individuals" and "electronically linked group of individuals" are so broad as to inadvertently draw within their ambit a swathe of individuals who happen to be legitimately using the same application (for instance, WhatsApp users who are electronically linked to individuals that are suspected of relevant offences, by virtue of using the same application),[25] potentially creating a chilling effect as to the work of journalists and their sources. These definitions should be narrowed to require that each individual in the group be engaged in or facilitating conduct that constitutes a relevant offence (whether knowingly or not). This would help protect the privacy of individuals who have no involvement in the criminal activity, while ensuring that law enforcement can target individuals or groups that inadvertently facilitate criminal activity, such as website administrators and app developers.

Further, there are avenues whereby a whistleblower can lawfully make a disclosure that may not necessarily be known until after the fact, during which time that person is wrongfully subjected to a

---

[19] *Surveillance Devices Act* s 27KM(2)(e).
[20] INSLM Issues Paper (n 10) [5.3].
[21] Ibid 36-8 [5.3]-[5.14].
[22] Ibid 37 [5.9].
[23] Ibid 42 [5.30].
[24] Ibid 30 [4.28].
[25] Evidence to Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, Canberra, 10 March 2021, 9 (Kieran Pender).

Network Activity Warrant. For example, the *Public Interest Disclosure Act* allows public servants to share information with a journalist in limited external disclosure circumstances.[26] This may give rise to a situation where a warrant is sought in relation to communications between a whistleblower and a journalist, even if that communication was ultimately conducted under lawful channels under the PID Act. This uncertainty and overreach only serve to stifle crucial components of our democratic processes.

Recommendation 3: The Warrants should only be available when other avenues of achieving the same results have been exhausted.

Recommendation 4: Both a new category qualifier and a heighted severity qualifier should be imported into the definition of "relevant offence".

Recommendation 5: The terms "criminal network of individuals" and "electronically linked group of individuals" should be narrowed to require that each individual in the group be engaged in or facilitating conduct that constitutes a relevant offence (whether knowingly or not).

4.3 Retention, analysis, use or disclosure

[6.16.1] Should there be an express requirement that the retention, analysis, use or disclosure of information obtained under warrants be necessary and proportionate?

The Centre's position regarding the handling of information collected under the Warrants aligns with that of the Parliamentary Joint Committee of Human Rights – namely, that a five-yearly review and destruction of data collected under these Warrants is not frequent enough.[27]

We acknowledge that the explanatory memorandum to the *SLAID Act* contemplates interference with the right to privacy in the context of both collection,[28] as well as use and disclosure,[29] and concludes that the processes pertaining to the new Warrants are justified. However, the explanatory memorandum glosses over the fact that the current regime's retention and disclosure provisions are particularly complex, as noted in the INSLM Issues Paper,[30] resulting in unnecessary uncertainty in an area that requires more, rather than less, clarify and precision.

Given the fact that *Privacy Act* obligations, which would ensure a more proportional approach to the handling of information, cannot be directly applied to certain intelligence agencies,[31] we recommend that clearer, more transparent overarching information handling practices, potentially mirroring those under the *Privacy Act*, are implemented to guide the handling of all information collected under this regime.

Recommendation 6: Clear processes regarding the handling of information collected under the Warrants should be implemented. These should include a requirement to review and destroy any information that is no longer relevant after a period of three years.

4.4 Public reporting

[8.8.1] Are the current public reporting requirements about SLAID powers appropriate?

As the INSLM Issues Paper notes, annual reports in relation to warrants under the *Surveillance Devices Act* to date do not include information regarding the number of arrests and prosecutions made pursuant to Data Disruption Warrants and Network Activity Warrants. This is despite the fact

---

[26] See, eg, *Public Interest Disclosure Act 2013* (Cth) ss 25, 26.
[27] Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Human rights scrutiny report* (Report No 1, 3 February 2021) 31-2 [1.71]-[1.72].
[28] Explanatory Memorandum, Surveillance Legislation (Identify and Disrupt) Bill 2021 (Cth) 5 [10].
[29] Ibid 6 [16].
[30] INSLM Issues Paper (n 10) 48 [6.7], 49 [6.13].
[31] *Privacy Act 1988* (Cth) ss 7(1)(f)-(g), (h); sch 1 s 6.2(e).

that the *Surveillance Devices Act* requires that this information be published in relation to any 'access under a warrant to data held in a computer'.[32]

This gap in reporting is occurring at the same time that news regarding the AFP's and ACIC's improper use of surveillance powers is beginning to surface.[33] Clear and unambiguous obligations to report on the number of Warrants that are requested and granted, and the number of arrests and prosecutions made pursuant to them, will go much further to ensuring public transparency – and ultimately the legitimacy – of these potent new powers by demonstrating whether their use is proportional to the aims sought.

Recommendation 7: Mandatory public report requirements in relation to arrests and prosecutions made pursuant to the Warrants should be enacted and made unambiguous.

4.5 Additional human rights measures

[9.16.1] Are there other measures not addressed elsewhere which are required in order to ensure that Australia complies with its international human rights and other obligations?

We note that several of the recommendations from the 2019 Comprehensive Review have been periodically implemented over the past few years in a series of National Security Legislation Amendments.[34] However, these amendments are yet to introduce key recommendations from the 2019 Comprehensive Review as they relate to warrants.

As noted in the 2019 Comprehensive Review:

> *[P]owers to covertly intercept and access communications, access computers and use surveillance devices are the most intrusive powers afforded to intelligence and law enforcement agencies in Australia. These powers should be subject to robust legal controls and safeguards that reflect fundamental legal and human rights principles, and that provide the public with confidence that these powers will only be used where they are necessary and proportionate to investigate serious matters.*[35]

Ultimately, we believe the best way that use of the Warrants can be made targeted and precise is to use every Australian's fundamental right to privacy as the key touchpoint. Appropriately affording this to every Australian should not be seen as unnecessary red tape. Indeed:

> *[H]uman rights have had a significant impact: not in preventing the use of valuable capabilities or powers, but in ensuring that their use is appropriately safeguarded. That impact is constitutional in nature. By requiring the State and its agencies to account to Parliament and to the courts, human rights law has ended the tradition of total executive control and transformed the national security landscape as it was [previously] understood […]*[36]

Fully implementing Recommendation 80 from the 2019 Comprehensive Review would not only serve to align with best practice as recommended in that review, but will also ensure that Australia better complies with its international human rights obligations by requiring that every Australian's right to privacy is qualified only when such a qualification is necessary and proportionate to legitimate goals being sought.

---

[32] *Surveillance Devices Act* s 50(1)(g)(ii), (i)(ii).
[33] Daniel McCulloch, 'AFP has "cavalier approach" to data powers', *The Canberra Times* (online, 28 April 2021) <https://www.canberratimes.com.au/story/7228800/afp-has-cavalier-approach-to-data-powers/>; Connor Pearce, 'Criminal intelligence agency may have unlawfully accessed information', *The Canberra Times* (online, 3 December 2024) <https://www.canberratimes.com.au/story/8836431/ombudsman-queries-acic-afps-use-of-surveillance-powers/?cs=14329&msg>.
[34] *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Act 2022* (Cth); *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 2) Act 2023* (Cth); *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 3) Act 2024* (Cth).
[35] 2019 Comprehensive Review (n 10) 266 [26.148].
[36] Anderson (n 9) 8 [27].

Recommendation 8: Recommendation 80 from the 2019 Comprehensive Review, namely that electronic surveillance should only be authorised where it is necessary for, and proportionate to, the purposes of an investigation, should be fully implemented.